UIC Law Review

Volume 40 | Issue 2 Article 12

Winter 2007

Identity Theft: Plugging the Massive Data Leaks with a Stricter Nationwide Breach-Notification Law, 40 J. Marshall L. Rev. 681 (2007)

Amanda Draper

IDENTITY THEFT: PLUGGING THE MASSIVE DATA LEAKS WITH A STRICTER NATIONWIDE BREACH-NOTIFICATION LAW

AMANDA DRAPER*

I. INTRODUCTION

Imagine running up the stairs in a hurry to catch the train you hear quickly approaching the station. Relieved to catch the train in the nick of time, and even more relieved to spot an open seat, you sit down and realize your backpack is unzipped. As your heartbeat is accelerating by the second, you frantically search inside to make sure nothing is missing. Then, in disbelief, you notice your wallet is gone. Just as you hurried to catch the train a moment earlier, you hurry to exit the train before it leaves the station to search for your missing wallet. It is, however, nowhere to be found. Someone has possession of your wallet, and that someone is likely going to use its contents to steal your identity.

While identity theft can occur through the theft of a person's wallet, it can also occur through a massive security breach. This Comment proposes that financial institutions and other businesses must promptly disclose to their customers when there has been a security breach and must shoulder the costs of that security breach. To fully explore this proposal, Part II of this Comment provides background information about identity theft[1] and its

* J.D., May 2007, The John Marshall Law School. The author wishes to thank her family for their encouragement and continuous support.

1. Identity theft is a growing problem in the United States, and Arizona is the identity theft capital of the United States. Jennifer Mulrean, *The Worst States for Identity Theft*, MSN MONEY, http://www.moneycentral.msn.com/content/banking/financialprivacy/p125094.asp (last visited Apr. 18, 2007). Nevada comes in second, followed by California, Texas, Colorado, Florida, New York, Washington, Oregon, and Illinois as the top ten worst states for identity theft. *Id.* Certain demographic trends such as a large elderly population that is not aware of the latest identity theft tactics and high methamphetamine use contribute to Arizona coming in at the top. *Id.* Additionally, in states where law enforcement officials are "cracking down on identity theft" and informing their citizens about it, there is an increased likelihood consumers will report the crime. *Id.*

numerous components, including examining the many consequences of several high profile customer data leaks.

Part III compares a range of federal legislation targeting identity theft, such as the Gramm-Leach-Bliley Act[2] and the Identity Theft and Assumption Deterrence Act of 1998,[3] and explains how the legislation is inadequate for dealing with the identity theft problem. Additionally, Part III compares various state legislation, such as Illinois legislation designed to safeguard consumers against identity theft.[4] It also closely examines new bills Congress is currently considering adopting as a way to prevent identity theft and protect consumers. Finally, Part III explores newly-available forms of biometric technology, such as a grocery chain's new index-finger scan,[5] as a way to safeguard against identity theft. Part IV then proposes that Congress adopt legislation placing the burden on businesses to prevent the leaking of private customer information as a means to further protect consumers from identity theft.

II. BACKGROUND

Identity theft[6] is the theft of personal or individual information, including a person's name, birth date, Social Security number, driver's license number, mother's maiden name, credit card numbers, or prior addresses.[7] It occurs when someone uses

2. *See* Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2000) (containing privacy policies and financial institutions' safeguards).

3. *See* Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028 (2000) (criminalizing fraud and other activities relating to "identification documents, authentication features, and information").

4. *See* Personal Information Protection Act, 815 ILL. COMP. STAT. 530/1-30 (2005); *see also* Press Release, Office of the Governor, Governor Blagojevich Signs New Laws Protecting Illinois Consumers from Identity Theft (June 16, 2005), *available at* http://www.illinois.gov//pressreleases/printpressrelease.cfm?recnum=4049 (discussing the enactment of a law making "Illinois the second state in the nation to require companies to quickly notify consumers in the state if their personal information is compromised due to a breach of company security").

5. *See* Dana Knight, *Grocery Chain Adds High-Tech Touch in Employee Recognition*, INDIANAPOLIS STAR, Aug. 16, 2005, at C1 (discussing how biometric identification systems, including fingerprints, handwriting, face recognition, voice recognition, and vascular patterns, are becoming more common in United States workplaces).

6. *See* Identity Theft Expert, http://www.realtysecurity.com (last visited Apr. 18, 2007) (providing numerous links to information and other resources that cover a wide range of current identity theft issues).

7. Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423, 1423 (2001); *see also* DAVID A. MAY & JAMES E. HEADLEY, IDENTITY THEFT 2 (David A. Schultz & Christina DeJong, eds., 2004) (stating that a clever criminal can take a person's Social Security number, credit card number, checking account number, or other confidential information to impersonate that person).

another person's personal information to commit fraud.[8] "Identity theft is one of the fastest growing crimes in the nation."[9]

The Federal Trade Commission ("FTC") received the highest number of customer fraud complaints in 2001, with identity theft accounting for forty-two percent of the 204,000 complaints entered into the FTC's Consumer Sentinel database in 2000.[10] Identity thieves stole personal information from an estimated 9.9 million Americans, according to a 2003 FTC survey.[11] Two-thirds of customer inquiries involved identity theft for Trans Union Corp., one of the three main credit bureaus.[12]

Identity theft is an attractive crime because an individual can commit identity theft easily and anonymously, such as by sorting through the trash or stealing someone's mail.[13] This includes the theft of pre-approved credit cards, the theft of items containing personal information found in garbage cans, dumpsters, or

---

8. William M. Savino, *Identity Theft and Insurance Coverage: Recent New York Decisions Offer Lessons for Insurers*, 9-8 MEALEY'S EMERG. INS. DISPS. 16 (2004). The regular daily activities of a consumer can provide an array of opportunities for an identity thief: purchasing gas, meals, clothes, gifts online, tickets to an event; renting a car, video, tools; retrieving mail; or simply taking out the trash or recycling. Hoar, *supra* note 7, at 1423. An opportunity is created for an identity thief anytime an activity in which identity information is shared or made available to others. *Id.*

9. Welcome to the State of California, Identity Theft — Office of Privacy Protection, http://www.privacy.ca.gov/cover/identitytheft.htm (last visited Apr. 18, 2007) (providing useful links to tips for identity theft protection).

10. Hoar, *supra* note 7, at 1423-24.

11. Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259, 261 (2005). Additionally, in the same survey, it was estimated that identity theft collectively cost businesses 47.6 billion dollars and cost consumers five billion dollars. *Id.* Furthermore, the Federal Trade Commission Identity Theft Survey showed an "exponential increase" in occurrences of identity theft, with the number of identity theft victims almost doubling each year for the previous two to three years. *Id.* at 261-62.

12. Hoar, *supra* note 7, at 1425. These inquiries "increased from an average of less then three thousand per month in 1992 to over forty-three thousand per month in 1997." *Id.* MasterCard International, Inc. and VISA U.S.A, Inc. reported that total losses from fraud reached hundreds of millions of dollars per year. *Id.* Additionally, in 1997, MasterCard reported losses due to identity theft that accounted for ninety-six percent of its total fraud losses. *Id.*; *see also* Ed Mierzwinski, News Release, The State PIRG Consumer Protection Inside Pages, Statement on MasterCard Security Breach Affecting up to 40 Million Cards (June 17, 2005), http://www.pirg.org/consumer/breach.htm (last visited Apr. 18, 2007) (noting that MasterCard's security breach demonstrates the "sloppy" ways companies handle confidential consumer information).

13. *See* Hoar, *supra* note 7, at 1424-25 (stating that identity theft can occur in a number of ways, from the sharing of personal information to the theft of purses, mail, wallets, and digital information); MAY & HEADLEY, *supra* note 7, at 15-17.

recycling bins, and the theft of new checks from a mailbox.[14] Additionally, identity theft can be committed using online or offline techniques.[15]

An identity theft victim will likely suffer devastating consequences.[16] In addition to monetary losses, victims can suffer "emotional distress from feeling personally violated by the theft, being harassed by creditors and collection agencies for debts they did not incur, being turned down for a loan or new account, or even being arrested for crimes committed by someone else in their name."[17]

A. The Growing Problem of Identity Theft

The illegal use of identity information has dramatically increased in recent years.[18] This is due, in part, to the widespread use of Social Security numbers as identifiers.[19] The exponential increase in identity theft is also due, in part, to massive data

---

14. Stephanie Byers, *The Internet: Privacy Lost, Identities Stolen*, 40 BRANDEIS L.J. 141, 143 (2001).

15. Lynch, *supra* note 11, at 262. Offline identity theft techniques include:

> pickpocketing, "dumpster diving" for discarded financial records and credit card statements, stealing pre-approved credit card applications from mailboxes, completing "change of address" forms through the Post Office to divert a victim's mail, and securing low-level employment with an organization to gain access to and steal consumers' SSNs, credit reports, and financial records.

Id. These offline techniques still make up the majority of identity theft cases; however, the Internet has played a large role in the dramatic increase of identity theft cases as well. *Id.* It is easier for identity thieves to gain access to more individual information all at one time due to the increased use of databases that store personal information. *Id.*

16. Hoar, *supra* note 7, at 1423. Often, victims of identity theft do not realize they have become victims until they attempt to obtain financing on a car or house. *Id.* at 1425. It is hard for a victim to realize that she has been victimized because the "fruits of an identity thief's crime take weeks, months, or even years to ripen." Anthony E. White, Comment, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who is Going to Pay for It?*, 88 MARQ. L. REV. 847, 850 (2005). *See* Lynch, *supra* note 11, at 260 (discussing that victims of identity theft suffer mainly financial losses; however, identity theft crimes also place a price on the victim in the time, money, and effort spent trying to rebuild his or her credit and good name, as well as a price on society in business losses passed on to consumers through higher costs for goods and credit). For businesses, financial losses to identity theft victims average 10,200 dollars per identity theft case, and for individuals, financial losses to identity theft victims average 1,180 dollars. *Id.* at 263.

17. Lynch, *supra* note 11, at 263-64.

18. *See* Hoar, *supra* note 7, at 1424 (stating that identity theft complaints accounted for forty-two percent of all FTC complaints in 2000, and that the Social Security Administration Office of Inspector General Fraud Hotline received around 62,000 allegations involving Social Security number misuse in 1999).

19. *Id.*

breaches at credit card processing companies and other firms and financial institutions.[20]

1. The Widespread Use of Social Security Numbers Adds to the Increasing Number of Identity Theft Cases

A chief piece of information desired by identity thieves is the Social Security Number.[21] In 1935, the government enacted the Social Security Act to "administer a federal government pension program".[22] Each person is assigned an individual account number, or Social Security number, composed of nine digits.[23] The first three digits of the Social Security number indicate the geographical area, the next two digits indicate the group, and the last four digits identify the individual's serial number.[24]

With the introduction of the Social Security number came the promise that it would not be used as "a national ID card."[25] The history of the creation of the Social Security number shows that it was not intended to be used as a general identifier. However, the increasingly widespread use of the Social Security number has made it just that.[26]

Currently, a person's Social Security number is the primary source for identification used by government agencies, schools, and financial institutions.[27] Identity thieves can use a person's Social Security number to gain access to bank accounts or medical records, which can then lead to the discovery of even more personal information.[28] An identity thief can open new bank

---

20. Charley Shaw, *ID Theft Remains on the Minnesota Legislative Agenda*, ST. PAUL LEGAL LEDGER, June 27, 2005, at 1.

21. White, *supra* note 16, at 853.

22. *See* S. Kasim Razvi, Comment, *To What Extent Should State Legislatures Regulate Business Practices as a Means of Preventing Identity Theft?*, 15 ALB. L.J. SCI. & TECH. 639, 644 (2005) (noting that as time went on, Congress authorized the use of Social Security numbers for reasons unrelated to the administration of social security).

23. Joseph L. Fay & Max J. Wasserman, *Bureau of Old-Age Insurance, Accounting Operations of the Bureau of Old-Age Insurance*, 1 SOCIAL SECURITY BULLETIN (June 1938), *available at* http://www.ssa.gov/history/fay638.html (last visited Mar. 15, 2007).

24. *Id.*

25. *See* Peter P. Swire, *Financial Privacy and the Theory of High-Tech Governmental Surveillance*, 77 WASH. U. L. Q. 461, 498 (1999) (examining the Department of Transportation's proposed rule to start using Social Security numbers as national identifiers). "The proposed rule would mandate that state driver's licenses must contain SSNs to be acceptable for a range of identification purposes, including boarding an airplane, being eligible for federal benefits, and purchasing a gun." *Id.* at 498-99.

26. White, *supra* note 16, at 853.

27. *Id.*

28. *Id.* When opening a new bank account, for example, an individual will likely have to disclose her Social Security number and other personal information. *Id.* The bank might end up selling that information to a third

accounts, open new credit card accounts, or apply for loans with that additional personal information combined with the Social Security number.[29]

2. Massive Data Breaches Complicate the Identity Theft Problem

The high profile security breaches at credit card processing firms and numerous other companies in 2005 have lawmakers thinking about new laws to protect consumers from identity theft.[30] Since February 2005, almost fifty million individuals have reported lost or stolen personal data from banks, colleges, hospitals, and other businesses.[31] Information brokers and banks are the main targets for identity thieves. However, any company that keeps customers' personal records is vulnerable to identity theft.[32]

A growing technique for identity theft is for thieves to become employed at financial institutions or other companies to gain access to confidential customer information.[33] As data storage

party institution and therefore, a person's Social Security number may be known by more institutions than the person would have originally expected. *Id.* This chain of events leads to the increasing vulnerability of an individual to potential identity theft simply by disclosing her Social Security number to a trusted institution in which she has knowledge of its sufficient security measures. *Id.*

29. *Id.*

30. Shaw, *supra* note 20, at 1; *see* Martha Neil, *Thinking Globally: Committee Begins to Address Electronic Privacy Issues on an International Scale*, 91 A.B.A. J. 62, 62-63 (2005) (stating that the recent chain of security breaches has raised concerns in Congress that thousands of people could become victims of identity theft); *see also* Wendy Toth, *Balanced Legislation — PCI Urges New York Senate to Pass Data-Security Legislation that Preserves the Use of Consumer Information*, INS. & TECH., Aug. 1, 2005, at 17 (acknowledging that policy makers have been prompted by the recent security breaches to address the use and collection of consumer information).

31. Kimberly Lankford & Christine M. Varner, *Beyond Shredders*, KIPLINGER'S PERS. FIN., Aug. 2005, at 1.

32. Jarrett Banks, *Identity Theft Suits Gain Popularity with Plaintiffs: General Counsel Brace for Increased Liability*, CORP. LEGAL TIMES, July 2005, at 32; *see also* Steven Levy & Brad Stone, *Grand Theft Identity*, NEWSWEEK, July 4, 2005, at 38 ("[I]t only makes sense that criminals would go where information is collected.").

33. White, *supra* note 16, at 851. Corporations are looking to secure their storage of personal information, but they have overlooked the major problem of insider data theft. Mike Saccone, *Little Devils*, CORP. COUNS., Oct. 2005, at 87. One of the largest incidents of data theft occurred at Bank of America Corp. in May 2005. *Id.* Seven employees of the company breached the account information of more than 670,000 customers. *Id.*; *see also* Mike Heck, *Guard Your Data Against Insider Threats*, INFOWORLD, Jan. 13, 2006, at 1 (providing information on insider threat management products which monitor communication channels and provide alerts and automatic remediation); *see also* GuardianEdge Techs., http://www.guardianedge.com (last visited Apr. 18, 2007) (providing valuable resources, support, and products about data

technologies advance, stealing massive amounts of personal consumer information is becoming much easier to do.[34] For example, in February 2005, ChoicePoint, Inc., a corporation that collects personal and financial data on millions of customers, accidentally sold the private data of 145,000 customers to identity thieves.[35] The ChoicePoint security breach led to at least 750 known cases of identity theft.[36] In April 2005, identity thieves took as many as 310,000 Social Security numbers contained in the LexisNexis database.[37]

---

protection to financial institutions and other businesses for implementation in their daily transactions).

34. *See* Saccone, *supra* note 33 (discussing how the use of USB thumb drives and other memory storage devices help people to store large amounts of data into smaller areas). Additionally, phones and PDAs are beginning to resemble mini computers as they gain more functions. *Id.* Thumb drives are dwarfed by smart devices, which can now hold up to sixty gigabytes of information. *Id.* Technological advances in data recovery are making digital data theft harder to track down. *Id.* Daniel Solove, the author of THE DIGITAL PERSON, stated:

> What's new is that we're seeing a rise in identity theft, a rise in demand for the data, a rise in the incentives to misuse the data, and a rise in the amount of data being collected. At the same time [we're still seeing] the pitiful level of security that existed before this information was hoarded by these companies.

Id.

35. *See* Banks, *supra* note 32 (noting that there is a lawsuit pending against ChoicePoint in California for accidentally selling personal customer information to identity thieves, in addition to a charge of "systematic and willful violation" of the Fair Credit Reporting Act and the California Credit Reporting Agencies Act); *Disclosure of Data Security Breaches*, STATE LEGISLATURES, Sept. 1, 2005, at 9, *available at* http://www.ncsl.org/programs/pubs/slmag/2005/05slsept_tandt.pdf (discussing how ChoicePoint became a victim of a security breach); Michael Sivy, *What No One is Telling You about Identity Theft*, MONEY, July 2005, at 94 (commenting on the compromised ChoicePoint data); *see also* Shari Claire Lewis, *Businesses Must Stay Ahead of Widening Range of ID Theft Scams*, N.Y.L.J., Apr. 12, 2005, at 5 (noting that Americans are the victims of identity theft every ten seconds, and that there are about 3.2 million incidents of identity theft each year); Denise Power, *Security Alert; New Customer Data Security Mandate Reaches Virtually All Online Retailers*, WWD, Mar. 9, 2005, at 9B (noting the serious risk of identity theft created by the ChoicePoint security breach); Damian Paletta, *'ChoicePointLaw' May Already Be Inevitable*, AM. BANKER, Mar. 9, 2005, at 1 (discussing various politicians' support of new regulations in light of the security breach by ChoicePoint).

36. *Disclosure of Data Security Breaches*, *supra* note 35.

37. *See* Banks, *supra* note 32 (stating that there could be a round of lawsuits against LexisNexis and "[t]here also will be a move in consciousness where people know this type of activity is illegal and Congress comes through and bumps up the penalties."); Lewis, *supra* note 35 (stating that unauthorized individuals took personal information from LexisNexis by stealing logins and passwords of customers); Sivy, *supra* note 35 (explaining that as many as 310,000 people had their personal information compromised by LexisNexis employees); *see also* Shaw, *supra* note 20 (reporting that after

Massive data leaks have become much more familiar in the last three or four years, but an early security breach occurred at Hallmark Cards, the greeting card vendor.[38] In 1998, Hallmark Cards discovered an error on its website that put the personal information of thousands of customers at risk.[39] However, the largest security breach by far occurred in May 2005, when CardSystems Solutions, which processes credit card information, revealed that a hacker gained access to the company's systems and stole data on forty million credit card accounts.[40]

Another security breach occurred when Bank of America lost thousands of its customers' personal data to identity thieves when it lost tapes containing personal information while being transported.[41] Furthermore, in May 2005 someone stole a laptop from MCI with the names and Social Security numbers of 16,500 employees.[42] Identity thieves stole 1.4 million names and credit card numbers from DSW Shoe Warehouse computers between February 2004 and March 2005.[43] CitiFinancial lost the personal financial information of 3.9 million customers in May 2005.[44] In March 2005, someone stole a computer containing personal information of 10,000 graduate students and applicants at the University of California at Berkeley.[45] These are just a few of the numerous instances where corporations, financial institutions, and

---

the massive security leaks at LexisNexis and ChoicePoint, the governor of Minnesota signed a bill that restricts the use of Social Security numbers).

38. David Eggleston, *Privacy Issues as Serious as Y2K*, STRATEGY, Sept. 13, 1999, at D11.

39. *Id.*

40. *Disclosure of Data Security Breaches*, *supra* note 35, at 9; Levy & Stone, *supra* note 32.

41. *Disclosure of Data Security Breaches*, *supra* note 35, at 9; *see also* Banks, *supra* note 32 (reporting that Bank of America lost data on potentially millions of clients, and that the company may face many lawsuits); Lewis, *supra* note 35 (noting the involvement of 1.2 million employees); Paletta, *supra* note 35 (reporting that the humiliating loss of information by Bank of America has led to a movement to crack down on security theft). The Bank of America security breach evidences the growing risk for identity theft. Wendy Toth, *Best Line of Defense — Insurers Are Under Immense Pressure to Keep Their Customers' Identities Safe. A Dynamic, Layered Approach to Security Technology May Provide the Strongest Protection*, INS. & TECH., Sept. 1, 2005, at 37; *see* Sivy, *supra* note 35, at 94 (noting the recent trend of major security breaches reported across the country).

42. Banks, *supra* note 32.

43. *Id.*; Tresa Baldas, *Capitol Hill, States Weigh Data Theft Notification Laws Even the Consumer*, PALM BEACH DAILY BUS. REV., May 11, 2005, at 11. A victim of the DSW Shoe Warehouse security breach stated: "It's scary . . . [p]art of it is the uncertainty that comes with it, not knowing whether sometime in the next year my credit-card number will be abused". Levy & Stone, *supra* note 32.

44. Levy & Stone, *supra* note 32; Toth, *supra* note 41; David Myron, *Online Banking: Consumer Trust Verses Loyalty*, CRM MAG., Sept. 1, 2005, at 12.

45. Levy & Stone, *supra* note 32; Sivy, *supra* note 35.

even schools to which individuals entrust their personal information have reported massive losses of customer information.[46] The problem has led to several bills pending in numerous states, as well as legislation in Congress related to data security that could ultimately preempt state laws.[47]

B. Identity Theft Prevention Techniques Are Not Adequately Dealing with the Problem

One way individuals can guard against identity theft is to protect their own personal information[48] by taking steps to limit potential vulnerability to identity theft.[49] For example, an individual should keep important documents, such as medical or financial records, in a safe place and shred receipts and anything else containing personal information instead of throwing them away.[50]

However, even the most diligent consumer may still be at risk of becoming the next victim of identity theft.[51] The "recent wave of personal data thefts" from companies all over the United States demonstrates the need for legislation to regulate how businesses

---

46. Marvin N. Bagwell, *Identity Theft Fraud is Alive and Well; in the Most Current Version, a Fake Buyer is Used to Do the Larcenous Transaction*, N.Y.L.J., Aug. 8, 2005, at 1.

47. *See* Shaw, *supra* note 20 (noting that in Minnesota, Governor Tim Pawlenty signed a bill that requires businesses to disclose security breaches to customers when their personal information is stolen and also signed a data practices bill that restricts the use of Social Security numbers). "Those laws were precipitated by disclosures by ChoicePoint Inc. in February and LexisNexis Inc. in March that personal information had been stolen." *Id.* The new restrictions in place in Minnesota prevent businesses from printing a customer's Social Security number on a card. *Id.* Nor can businesses require a customer to give her Social Security number over the Internet unless the site is secure or encrypted, and customers may only be required to use their Social Security number to access a site if a personal identification number is also required. *Id.*

48. White, *supra* note 16, at 854-55.

49. *See id.* at 855 (discussing how an individual could store or dispose of documents containing personal information with special care, as a way to protect herself from identity theft). One list of the top ten ways to prevent identity theft includes: destroy private records, secure your mail, safeguard your Social Security number, do not leave a paper trail, keep track of your credit cards, become familiar with who you are dealing with, take your name off marketers' lists, become more defensive with your personal information, monitor your credit report and review your credit card statements very carefully. Jeff Wuorio, *Ten Ways to Stop Identity Theft Cold*, MSN MONEY, http://moneycentral.msn.com/content/banking/financial privacy/P33715.asp (last visited Apr. 18, 2007).

50. Following these steps can reduce the chance of identity thieves finding personal or confidential information and using it to the detriment of the victim. Wuorio, *supra* note 49.

51. Baldas, *supra* note 43.

safeguard customer information.[52] The most careful consumer may still end up the victim of identity theft if businesses and financial institutions continue to be careless in their handling of customer information.[53]

III. ANALYSIS

Identity theft is an easy crime to commit, and its effects on a victim can be devastating.[54] Identity theft has cost Americans at least five billion dollars, and the average victim spends over six hundred hours and $1,400 trying to fix damaged credit.[55]

The federal legislation aimed at preventing identity theft does not adequately protect consumers. A few states, such as California and Illinois, have enacted new legislation which helps to close the gaps found in federal legislation. Additionally, bills currently going through Congress could, however, increase the likelihood of preventing identity theft.

A. Current Federal Legislation is Not Fully Protecting Consumers from Identity Theft

1. The Identity Theft and Assumption Deterrence Act of 1998[56]

President Clinton signed the Identity Theft and Assumption Deterrence Act of 1998 ("ITADA") into law on October 30, 1998.[57] Under the ITADA, it is unlawful for a person to "knowingly transfer[] or use[], without lawful authority, a means of identification of another person with the intent to commit, or to

52. *See id.* ("Consumers are suing companies for being careless with their personal data, causing it to get lost or stolen, and triggering fears of identity theft.").

53. *Talk Transcript: Identity Theft — Newsweek Business*, MSNBC, June 30, 2005, http://www.msnbc.msn.com/id/8357784/site/newsweek (last visited Apr. 18, 2007).

54. *See* White, *supra* note 16, at 848 (discussing the need for courts to recognize a cause of action for victims of identity theft against financial institutions whose negligence in establishing sufficient computer security lets an identity thief gain the victim's personal information and use that information to the detriment of the victim).

55. *Id.*

56. 18 U.S.C. § 1028.

57. Kristen S. Provenza, *Identity Theft: Prevention and Liability*, 3 N.C. BANKING INST. 319, 324 (1999). The "ITADA considers the victim to be the person whose identity was stolen and allows sentencing enhancements based on number of victims and harm done to his or her reputation." Lynch, *supra* note 11, at 294; *see also* The Honorable Diana E. Murphy, *Sentencing Symposium: The United States Sentencing Commission: Starting up Again*, 44 ST. LOUIS L.J. 279, 287 (2000) (noting that the key change in the ITADA was to "expand the scope of victims affected by these offenses to include those individuals whose identification information may have been misused, not just the financial institutions").

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."[58]

The ITADA's purpose is to fill in the gap in federal law that allowed an identity thief to steal information from financial institutions in order to steal the identities of individuals without being pursued by law enforcement officials in the early stages of the act.[59] The act of stealing the information with the intent to commit a fraud is a crime under the ITADA, as opposed to the required use of that information to commit a fraud under the previous Credit Card Fraud Act; therefore, law enforcement officials can begin an investigation earlier.[60] Further, the ITADA criminalizes identity theft and imposes penalties of imprisonment up to fifteen years, as well as fines.[61]

However, the ITADA fails "to regulate the exchange and dissemination of personal data prior to its theft or misuse."[62] The ITADA does not address the problems that come with the wide availability of personal information obtained on the Internet.[63] Additionally, the ITADA does not provide any true remedy to victims, because federal law prohibits courts from awarding restitution to the victims for costs associated with identity theft.[64]

2. *The Gramm-Leach-Bliley Act*[65]

The Gramm-Leach-Bliley Act ("GLBA") requires federal banking agencies to establish safeguards for financial institutions to ensure the confidentiality and security of consumer information, protect against threats to the security of personal records, and protect against unauthorized access to confidential personal information.[66] The GLBA "prohibits a person from using false pretenses to obtain financial information from a customer."[67] However, it authorizes financial institutions to share certain

58. Michael W. Perl, Comment, *It's Not Always About the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft*, 94 J. CRIM. L. & CRIMINOLOGY 169, 183 (2003).

59. *Id.*; *see* Catherine Pastrikos, *Identity Theft Statutes: Which Will Protect Americans the Most?*, 67 ALB. L. REV. 1137, 1140 (2004) (noting that the ITADA criminalizes the use of both public and non-public information).

60. Lynch, *supra* note 11, at 294.

61. Byers, *supra* note 14, at 152.

62. *Id.* (internal quotation marks omitted).

63. *Id.*

64. Janice A. Alwin, *Privacy Planning: Putting the Privacy Statutes to Work for You*, 14 DEPAUL BUS. L.J. 353, 364 (2002).

65. 15 U.S.C. § 6801.

66. *Arkansas Amends Mortgage Law*, CONSUMER FIN. SERVICES L. REP., May 18, 2005, at 15.

67. Lynch, *supra* note 11, at 265.

private personal information with their agents, affiliates, and other third parties.[68]

The mechanisms in place for the GLBA are not effective in protecting customers from identity theft.[69] The law requires financial institutions to implement security measures to protect consumer data, but it does not specify what measures they should take or what the penalty is for failure to comply.[70] It also does not give consumers a private cause of action.[71] The GLBA only covers financial institutions, so all other firms are exempt from the above criteria.[72] In addition, the GLBA does not prohibit financial institutions from disclosing non-public information about a customer to their affiliates even if the customer wants to keep this information private.[73]

3. *The Fair and Accurate Credit Transactions Act of 2003*[74]

In December of 2003, President George W. Bush signed into law the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which governs the disposal of financial information under the Fair Credit Reporting Act ("FCRA"). Its purpose is to protect information from being used for identity theft.[75] FACTA covers customer credit reports and requires due diligence and monitoring by the institutions of the entities chosen to dispose of the personal information.[76] Unlike the GLBA, which only covers financial institutions, FACTA also includes credit reporting agencies.[77]

FACTA places the burden of detecting identity theft and clearing up the problem on the victim, and it does not provide

68. Alwin, *supra* note 64, at 361. The information that can be shared by financial holding companies is divided into five types: information that the customer provided on an application for credit, information collected from a credit-reporting agency, information obtained from outside sources as verification of customer representations, information collected and accumulated as a result of daily account transactions, and any general information, including demographics, that was used to determine credit eligibility. *Id.*

69. White, *supra* note 16, at 861.

70. *Id.*; *see also Legal Identity Theft: The Newest HR Challenge*, HRFOCUS, June 2005, at 1 (discussing the GLBA and its effect on how consumers choose service providers to handle their personal data and how those service providers handle the security of their personal information).

71. *Legal Identity Theft: The Newest HR Challenge*, *supra* note 70.

72. Paletta, *supra* note 35.

73. Alwin, *supra* note 64, at 362.

74. Pub. L. No. 108-159, 117 Stat. 1952.

75. *Legal Identity Theft: The Newest HR Challenge*, *supra* note 70.

76. *Id.*

77. Paletta, *supra* note 35.

automatic credit reports, only providing free credit reports once a year.[78] This may not be enough to detect the fraud.[79]

The Supremacy Clause of Article VI of the United States Constitution provides that "if there is any conflict between federal and state law, federal law shall prevail."[80] Federal law preempts state law in three different instances: first, when Congress expressly defines the extent to which federal law preempts state law; second, when state law regulates in a field exclusively intended for Congress to occupy; and third, when state law and federal law actually conflict.[81] As a result, FACTA, like other federal statutes, may preempt state statutes which provide broader protections to customers if they are inconsistent with a provision of FACTA.[82]

B. California and Illinois Are Paving the Way in Establishing Identity Theft Prevention Statutes

California[83] enacted its data theft disclosure law in 2003,[84]

---

78. Lynch, *supra* note 11, at 280; *see* Kevin DeMarrais, *The Record, Hackensack, New Jersey, Your Money's Worth Column*, KNIGHT-RIDDER TRIB. BUS. NEWS, Aug. 28, 2005, at 1 (stating that FACTA mandates that free credit reports be made available to customers across the country, starting with the West Coast in December 2004, the Midwest in March 2005, the South in June 2005, and the Northeast in September 2005).

79. Lynch, *supra* note 11, at 280; *see also* Paletta, *supra* note 35 (examining the federal government's difficulty in passing effective legislation). FACTA required seven rules to be in effect regarding identity theft, and only three have been completed. *Id.* The three rules that are in place now define identity theft, provide a summary of identity theft victims' rights, and require companies to destroy various unused personal customer data. *Id.* The four left would help banks determine when identity theft has occurred, create a system for victims to report crimes, make it easier for customers to dispute credit information if they think they have been a victim of identity theft, and instruct banks and credit agencies about how to handle customers with conflicting addresses, which is a known indicator of identity theft. *Id.*

80. Gonzales v. Raich, 545 U.S. 1, 29 (2005).

81. Tina M. Parker, *Preemption in Automotive Crashworthiness Cases: Post-*Geier v. American Honda Motor Co., 67 ALA. LAW 118, 119 (2006).

82. Lynch, *supra* note 11, at 280-81; *see also* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 380 (2006) (noting that the FRCA, the predecessor to FACTA, also preempted more protective state laws).

83. *See* Baldas, *supra* note 43 (stating that California's law has not only led to the disclosure of company security breaches, but has also influenced legislation in other states); Levy & Stone, *supra* note 32 (maintaining that the reason people are hearing about the numerous security breaches is because of the 2003 California law requiring, for the first time, that companies disclose the failures that affect the residents of that state, stating "[t]he general public is just now learning about how insecure the computer networks are that hold our sensitive personal information"); Allan Holmes, *Riding the California Privacy Wave*, CIO MAG., Jan. 15, 2005, at 1 (stating that California is where everyone looks for the trends, including legislation, and that the California state legislature has enacted more than a dozen laws regulating how

and it was the only such law in the country at that time.[85] California's law requires companies to promptly notify all state residents if identity thieves steal their personal information, or if information disappears.[86] California's law has led to the disclosure of many security leaks, such as the notification of the security breach at ChoicePoint, while also influencing legislation in other states.[87]

In California, any individual, not just an identity theft victim, can place a "security freeze" on her credit history.[88] A security freeze makes it nearly impossible for identity thieves to make unauthorized applications for credit because it makes it hard for merchants and other credit providers to review an applicant's credit history without permission.[89] Additionally, companies handling personal information of California residents must "implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[90]

On June 16, 2005, Illinois Governor Rod R. Blagojevich signed into law several pieces of legislation designed to protect Illinois consumers against identity theft.[91] These acts place rigid regulations on businesses, including requiring them to quickly notify customers of possible security breaches, increasing the penalties against identity thieves, and providing victims with resources to protect themselves from further violations.[92]

The Personal Information Protection Act requires any entity that gathers personal data to promptly notify customers affected by a security breach.[93] House Bill 1058 allows victims of identity theft to place a security freeze on their credit report.[94] Senate Bill

---

businesses, universities, and other organizations that collect personal information on its residents must handle that private information).

84. Baldas, *supra* note 43.

85. *Id.*

86. *Id.*

87. *See* Sivy, *supra* note 35 (noting that California has the nation's most stringent privacy laws and that without them the security breaches at LexisNexis or ChoicePoint, where the company first only disclosed the breach to California residents as required by the law, may have never been known).

88. Dean Foust, *Keeping a Grip on Identity; How to Hold Info Brokers Accountable for Security Without Fouling Up Commerce*, BUS. WK., Mar. 28, 2005, at 34 (noting the ability of consumers in California and Texas to protect their identity).

89. *Id.*

90. Power, *supra* note 35.

91. Press Release, Governor Blagojevich Signs New Laws Protecting Illinois Consumers from Identity Theft, *supra* note 4.

92. *Id.*

93. *Id.*; H.R. 1633, 94th Leg. (Ill. 2005).

94. Press Release, Governor Blagojevich Signs New Laws Protecting Illinois Consumers from Identity Theft, *supra* note 4; *see* H.R. 1058, 94th Leg. (Ill. 2005). The bill prevents the release of a credit report to anyone without the person's consent, prevents a thief from opening further credit card accounts

1799 was also signed into law, and requires the Department of Revenue to directly notify taxpayers if it suspects another person has used their Social Security number.[95]

Other bills include Senate Bill 123, requiring the Illinois Department of Natural Resources to phase in new Conservation ID numbers to replace Social Security numbers on hunting and fishing licenses;[96] House Bill 2696, prohibiting businesses from denying a person utility services or credit based only on that person's status as an identity theft victim;[97] House Bill 2697, making the unauthorized copying of any financial transaction a Class A misdemeanor;[98] and House Bill 2699, increasing the penalties by one felony class for identity theft crimes.[99] Congress too is now taking steps and examining proposed federal legislation to enhance identity theft protections.

---

with the person's information, and prevents a thief from changing personal information on credit reports. H.R. 1058.

95. Press Release, Governor Blagojevich Signs New Laws Protecting Illinois Consumers from Identity Theft, *supra* note 4; S.R. 1799, 94th Leg. (Ill. 2005).

96. Press Release, Governor Blagojevich Signs New Laws Protecting Illinois Consumers from Identity Theft, *supra* note 4; *see* S.R. 123, 94th Leg. (Ill. 2005). The bill still requires the DNR to keep a record of the Social Security number on file, even though it will not appear on the license. S.R. 123.

97. Press Release, Governor Blagojevich Signs New Laws Protecting Illinois Consumers from Identity Theft, *supra* note 4; *see* H.R. 2696, 94th Leg. (Ill. 2005).

98. Press Release, Governor Blagojevich Signs New Laws Protecting Illinois Consumers from Identity Theft, *supra* note 4; *see* H.R. 2697, 94th Leg. (Ill. 2005).

99. Press Release, Governor Blagojevich Signs New Laws Protecting Illinois Consumers from Identity Theft, *supra* note 4; H.R. 2699, 94th Leg. (Ill. 2005). According to Consumers Union, as of June 27, 2006, thirty-one states, including California and Illinois, have passed and/or signed into law various security breach state laws. Consumers Union, *Notice of Security Breach State Laws*, June 27, 2006, http://www.consumersunion.org/campaigns/breach_laws_may05.pdf (last visited Apr. 18, 2007). The states passing security breach state laws include: Arkansas, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Washington, and Wisconsin. *Id.* For example, Louisiana's bill requires notice of a breach of "the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons doing business in the state." *Id.* However, no notice is required if, "after a reasonable investigation, the holder of data concludes that there is no reasonable likelihood of harm to consumers." *Id.* Additionally, Washington's law requires "notice of a breach in security, confidentiality, or integrity of unencrypted, computerized" information belonging to individuals, businesses, or government agencies. *Id.* However, "notice is not required if there is a technical breach of the security of the system which does not seem reasonably likely to subject consumers to risk of criminal activity." *Id.*

C. Congress Could Enhance Identity Theft Protection Through New Legislation

Identity theft is a nonpartisan issue, its victims live in every state, and Congress is starting to take action.[100] Moving through Congress are various bills to protect the confidentiality of Social Security numbers.[101] For example, the purpose of the Social Security Number Privacy and Identity Theft Prevention Act of 2005[102] is to enhance Social Security account protections, prevent misuse of the Social Security number and generally enhance protection against identity theft.[103]

Additionally, there are also bills going through Congress dealing with data security.[104] On July 28, 2005, the Senate Commerce Committee approved the Identity Theft Prevention Act,[105] which explains how corporations are to handle consumers' information.[106] The Identity Theft Prevention Act would require non-financial companies, such as data brokers, that handle personal customer data to ensure its security by using safeguards specified by the FTC.[107] This might not address the full scope of the identity theft problem though, because it does not require financial companies that handle personal information to

---

100. *See* Banks, *supra* note 32 (quoting Kevin D. Lyles, a partner at Jones Day: "[a] couple more headline cases and I think Congress will step in").

101. *Arkansas Amends Mortgage Law*, *supra* note 66.

102. H.R. 1745, 109th Cong. (2005).

103. *Arkansas Amends Mortgage Law*, *supra* note 66. Additionally, the purpose of The Social Security Number Misuse Prevention Act, H.R. 637, 108th Cong. (2003), is to limit the misuse of Social Security numbers and establish criminal penalties for their misuse. *Arkansas Amends Mortgage Law*, *supra* note 66.

104. *See* Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong.; Identity Theft Prevention Act, H.R. 220, 109th Cong. (2005); *see also* Paula J. Hane, *Information Privacy Forum; Data Security*, INFO. TODAY, Sept. 1, 2005, at 1 (noting that the Personal Data Privacy and Security Act, introduced by Senator Patrick Leahy of Vermont and Senator Arlen Specter of Pennsylvania, is currently under consideration in Congress, and that the Identity Theft Prevention Act was the tenth identity theft bill introduced in Congress last session).

105. S. 1408, 109th Cong. (2005); *Legislative Update*, AM. BANKER, Aug. 11, 2005, at 5. Senator Gordon Smith of Oregon, Senate Commerce Chairman Ted Stevens of Alaska and Senator Daniel Inouye of Hawaii sponsored the bill. *Id.*

106. *See id.* (stating that jurisdictional conflicts over the bill with the Judiciary Committee and Senate Banking Committee have to be resolved before the bill can be considered in the full Senate); *see also* Hane, *supra* note 104 (noting that there is a need to strike a balance between consumers' rights to privacy and marketers' rights to conduct business transactions).

107. Hane, *supra* note 104; *see also* Steven Marlin, *Congress Responds to Data-Security Fears — Legislation Would Mandate Data-Security Programs and Consumer Notification*, INFO. WK., July 4, 2005, at 26 (stating that the legislation addresses the growing public concern about identity theft).

implement the FTC's safeguards.[108] However, if a company concludes that a security breach creates a reasonable risk of identity theft, the company must notify its customers or face fines of up to $11,000 per customer.[109] The legislation also allows consumers to put a freeze on their credit reports.[110] As previously noted, this bill preempts conflicting state laws.[111]

D. Biometric Technology Could Greatly Increase Consumer Protection Against Identity Theft

Biometric data is a technique used to identify individuals based on unique physical characteristics.[112] Biometric data includes fingerprints, hand imaging, retinal scans, voice recognition, and other personal physical traits.[113] Currently, grocery stores,[114] banks, and workplaces are using biometric data to improve security.[115] Increasing and expanding the use of biometric data helps to prevent identity theft, as biometrics rely on machines, not humans.[116] Since identity theft is the fastest growing crime in America, federal and state legislatures are continuously challenged to fight it effectively.[117] Biometric data can ensure security in a variety of settings and prevent data from getting into the wrong hands and eventually causing security breaches.[118] Requiring a thief to provide a retinal scan rather than a mother's maiden name, for example, would make it much harder to steal identities.[119]

IV. PROPOSAL

The government did not intend Social Security numbers to become nationwide identifiers, but that is precisely what they have become.[120] Until a new federal law is passed to restrict the

---

108. Marlin, *supra* note 107.
109. Banks, *supra* note 32.
110. *Id.*
111. *Id.* The bill would allow financial services companies to keep operating under the breach-notification rules of the GLBA. *Id.*
112. Perl, *supra* note 58, at 204.
113. *Id.*
114. *See* Knight, *supra* note 5 (discussing how Kroger, a local grocery store in Indianapolis, added a fingerprint scan to clock employees in and out).
115. *See* Perl, *supra* note 58, at 205 (noting that airports also plan to add biometric technologies to improve their security). As the devices that are needed to scan biometric information become more easily available, some predict the devices will soon be installed on personal computers. *Id.*
116. *Id.*; MAY & HEADLEY, *supra* note 7, at 62.
117. Perl, *supra* note 58, at 206.
118. *Id.* at 205.
119. MAY & HEADLEY, *supra* note 7, at 63.
120. *See id.* at 12 (noting that, beginning in 1943, the ease and usefulness of a "single and unique numerical identifier" became clear, and the mandated uses for the identifier began to increase).

use of Social Security numbers, there is not much one can do about their widespread use.[121] Even if implementing biometric data into everyday activities becomes prevalent, the problem of identity theft will still exist due to company security breaches. People voluntarily give out their personal information to companies who fail to adequately safeguard that information.[122]

The problem of identity theft has gotten out of hand.[123] "[I]nstead of losing our identities one by one, we're seeing criminals grabbing them in massive chunks — literally millions at a time."[124] According to a 2005 study by Yankelovich, a market research firm, "many Americans believe strengthening privacy safeguards" should be the government's number one priority.[125] Companies and financial institutions are simply not taking the necessary steps to safeguard personal customer information. They leave the information unencrypted on computers where hackers can get a hold of it, inadvertently sell information to thieves, leave information on laptops which are stolen, or they do not monitor what insiders do with the information.[126] Whatever the case may be, the ramifications that companies face for leaking consumer data need to be clearly set out in order to force them to implement stricter guidelines on how to protect it.[127]

Currently, the Identity Theft Prevention Act is the only federal legislation seeking to protect consumers from identity theft due to company security breaches. As previously noted, however,

---

121. The regulation of Social Security numbers may be a proper exercise of government power within the Commerce Clause because they may exist within databases "sold in interstate commerce." Justice Lebedeff, *Decision of Interest; New York County Supreme Court; on Legal Authority for Demand, Social Security Numbers Are Subject to Privilege Against Disclosure*, N.Y.L.J., Mar. 9, 2005, at 18.

122. Paletta, *supra* note 35.

123. Levy & Stone, *supra* note 32.

124. *Id.* The new worries about identity theft have led people to restrict their activities and be extra careful with their credit cards and other personal information. *Id.* Identity theft can be analogized to bank robbery: just as a bank robber robs a bank because that is "where the money is," an identity thief goes to a company databank because that is where names, Social Security numbers, credit card numbers, financial information and other confidential consumer information can be found. *Id.* Then, the identity thieves turn that information into cash by selling it to "fraudsters," who will use that information to impersonate other people. *Id.* However, since a modern identity thief commits the crime remotely, the thief is likely to suffer little of the risk that a bank robber traditionally would have suffered. *Id.*

125. Holmes, *supra* note 83. The rise in identity theft has made consumers skeptical of corporate efforts to collect confidential consumer data. *Id.*

126. Levy & Stone, *supra* note 32. Various recent company data leaks have taken many different forms. *Id.*

127. *See* Hane, *supra* note 104 (stating, as an example, that companies need to have a security policy in place, better train their employees, supervise their security, use the latest technology, and constantly update procedures).

it does not adequately protect consumers. Congress must amend this law or enact a new law to put a stop to massive data leaks.

A new federal law should require all businesses that engage in interstate commerce, as well as financial institutions and health care companies, to promptly notify all of their nationwide customers of possible data leaks of any personal information, including information contained on the Internet. Furthermore, companies should be required to notify their consumers of any risk of fraud, even a minimal risk.

The new law should also impose strict requirements on how companies handle their confidential data, such as making it illegal to send out information in the mail or online containing a person's Social Security number, not allowing companies to share their personal customer data with their affiliates, or placing tighter controls on the granting of credit. If companies do not comply with these requirements, then the law must impose severe penalties. Penalties could include increasing existing monetary fines, allowing consumers private causes of action, or providing automatic credit reports for all customers. Additionally, Congress should expressly define in its new law that it preempts all inconsistent state laws so as to preempt all state laws that do not offer enough consumer protection.[128]

The new law must apply to all businesses. The Identity Theft Prevention Act exempts financial institutions and some health care companies, because they are already covered under existing laws, such as the GLBA.[129] It also requires companies to notify their customers only if a security breach creates a reasonable risk of identity theft.[130] In order for the law to effectively protect consumers, the standard for notification must be one of possible data leaks. The reasonable risk requirement is not enough because identity theft is a problem that needs to be dealt with right away before the harm becomes too great for the consumer to fix.[131]

Last, the new law must apply to all kinds of customer data, including data contained on the Internet. Companies continue to conduct more and more business on the Internet. A number of security breaches have occurred by thieves exploiting confidential data on the Internet. Therefore, this type of information cannot be exempted from the new law.

---

128. *See* U.S. CONST. art. VI, cl. 2. ("[T]he Laws of the United States . . . shall be the supreme Law of the Land.").

129. Marlin, *supra* note 107.

130. *Id.*

131. *See* MAY & HEADLEY, *supra* note 7, at 3 (noting that since identity theft is such a complex crime, it is hard for the criminal justice system to track it).

As of June 27, 2006, thirty-one states have enacted disclosure laws.[132] Some of them offer broader protections than the Identity Theft Prevention Act, which could preempt the state disclosure laws, thus losing some of their protections.[133] However, some of them offer less protection in that they only require notice to consumers of a material breach or if the breach is likely to result in harm to the victim.[134] The thirty-one states that have enacted disclosure laws differ to the extent that consumers who do business in more than one state will not be aware of the differing protections.[135] Also, many of the state laws only require companies to notify the residents of that state if their personal information is stolen. As people continue to conduct more and more business nationwide, the statewide notification requirement becomes obsolete.

The current federal law exempts companies from notifying consumers of a security breach if it conducts a risk assessment with law enforcement and concludes the risk of fraud is minimal.[136] However, when dealing with identity theft, any risk of fraud, even minimal risk, should be enough for notification. The most essential goal is "to make consumer data useless once it falls into the hands of thieves."[137] Stricter guidelines would encourage companies to strengthen their own security programs.[138] A stricter

---

132. *Notice of Security Breach State Laws*, *supra* note 99.

133. *Id.*

134. *See id.* For example, Florida House Bill 481 only requires companies to notify their consumers of a material breach, and Senate Bill 650 does not require disclosure if after consultation with federal, state and local law enforcement agencies, the breached entity determines that the breach is not likely to result in harm to the individuals. *Id.*

135. *Id.*

136. *See* Marlin, *supra* note 107 (noting that the "fraud-prevention exemption" does not require companies to notify their customers if compromised data cannot be used to commit fraud, or if the company implements a security program that is reasonably designed to block the use of fraudulent transactions).

137. Michele Heller & Isabelle Lindenmayer, *Security Watch*, AM. BANKER, Sept. 23, 2005, at 5. For example, Visa is requiring more merchants to have "vigorous" audits and is creating websites giving approved software applications and service providers; thus, vendors can check the lists before installing a program. *Id.* Visa planned to hold its first security summit on October 5, 2005, in Washington. *Id.* MasterCard International's president focused on a different aspect of controlling security breaches: notification. *Id.* As Ruth Ann Marshall, the president, said, "If protecting customer data is paramount, then notifying customers of any breach becomes paramount, as well." *Id.*

138. *See* Holmes, *supra* note 83 ("Like a large hurricane sweeping in off the Pacific, these laws will wreak havoc on all kinds of business processes, including how websites can collect personal data and the management of databases that store personal information on customers."). However, complying with these laws could be good for business. *Id.* The senior vice

law will influence every aspect of businesses and how they share personal data with third parties.[139]

It is, nevertheless, crucial to find the right balance between securing consumer data without irrevocably harming the industry.[140] The proposed law strikes the proper balance between the two competing interests. The proposed measures protect the consumer's privacy by affording the consumer an option of attempting to fix the problem before it is too late, without restricting a company's right to conduct business efficiently. If a company has the proper safeguards in place, then the risk of identity theft is almost completely removed.

Attempting to clean up data leaks is extremely expensive,[141] so avoiding the problem entirely would save time and money. The costs to the industry are overwhelming.[142] Companies incur substantial losses when someone creates false credit accounts or uses forged checks.[143] The proposed law avoids placing these losses on the consumer or business entirely. The costs of creating the safeguards far outweigh the loss of a company's goodwill, time and money when a massive data leak occurs.

V. CONCLUSION

Identity theft is a nationwide problem. Current federal and state laws cannot adequately deal with the increasing problem of identity theft.[144] Even the most diligent consumer, who protects her own private data by checking credit reports, shredding bills,

---

president and CIO for Lands' End said, "These laws are not constraining our ability to do business . . . . It's to the benefit of our customers." *Id.*

139. *See id.* (discussing how these laws could also restrict a company's ability to contact consumers via cell phones and faxes and could also affect how a company outsources services that handle confidential information).

140. *See* Foust, *supra* note 88 (noting that striking a balance between privacy interests and industry interests will be very tricky); *see also* Hane, *supra* note 104 (discussing the need for a balance between consumers' right to privacy and marketers' right to conduct business).

141. *See* Foust, *supra* note 88 (stating that in 2003 the FTC estimated that annual losses from identity theft were about 47.6 billion dollars).

142. MAY & HEADLEY, *supra* note 7, at 38.

143. *See id.* at 38-39. The business losses attributable to identity theft consist of direct fraud losses, loss avoidance costs, and indirect costs. *Id.* Direct fraud losses are the losses incurred when someone uses false information to open false accounts. *Id.* at 38. "Loss avoidance costs include staffing of fraud hotlines and customer education as well as interdiction and investigation of possible fraud." *Id.* at 39. Indirect costs are those "as a result of loss of consumer confidence in the credit system" that could lead to consumers "opting out" of the credit system or using it less frequently. *Id.* Fraud prevention and resolution also requires credit providers and financial institutions to incur additional costs for employing fraud departments and dispute resolution services. *Id.* at 40. Other expenses include increased customer relations expenses as a result of the identity theft. *Id.*

144. Alwin, *supra* note 64, at 354.

and staying away from Internet transactions asking for Social Security numbers, remains at risk as a result of companies failing to safeguard that data.[145] Congress must consider amending its laws to shift the burden to the breaching company and make it liable for leaking consumer data. A federal law in line with the above proposal would address the public's growing concern about the biggest problem of identity theft, massive data leaks, without restricting business too severely.

145. *Talk Transcript: Identity Theft — Newsweek Business*, *supra* note 53. Maria Bruno-Britz, *Preventing Identity Theft — Maximum Security — Banks, Vendors and the Government Strategize on Ways To Foil ID Thieves*, BANK SYS. & TECH., Sept. 1, 2005, at 37.