Loyola Consumer Law Review

Volume 18 | Issue 3 Article 2

2006

Identity Theft, Its Environmental and Proposals for Change

Gary M. Victor
Prof. Dept of Marketing & Law, College of Business, Eastern Michigan University

FEATURE ARTICLES

Identity Theft, Its Environment and Proposals for Change

By Gary M. Victor*

Introduction

"Identity (ID) theft[1] is the use of another individual's personal information for fraudulent purposes.[2] The ID thief typically steals the victim's credit in order to obtain cash, goods or services.[3] As early as

---

* Mr. Victor is a sole practitioner specializing in Consumer Law and is "Of Counsel" to Lyngklip & Taub Consumer Law Group PLC, Southfield Michigan. Mr. Victor is also a professor in the Department of Marketing and Law in the College of Business at Eastern Michigan University. He is a council member of the State Bar Consumer Law Section and was selected by the council to be the second recipient of the Frank J. Kelly Consumer Advocacy Award. He has litigated several landmark consumer law cases and has written many articles on consumer law and related topics.

[1] For an interesting and, at times, humorous book on ID theft and other credit issues, see Steve Weisman, 50 WAYS TO PROTECT YOUR IDENTITY AND YOUR CREDIT (Pearson Education, Inc., 2005).

[2] The Federal Trade Commission defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." Fair Credit Reporting Act, 16 C.F.R. § 603.2(a) (2005).

[3] This can be thought of as "financial" ID theft. Two other less common types of ID theft are "criminal" ID theft—where the personal information is often used to avoid criminal liability and "identity cloning"—where someone takes over another's identity to establish a new life. *See* Identity Theft Resource Center, *Identity Theft—The Aftermath 2003: A Comprehensive Study—to Understand the Impact of Identity Theft on Known Victims as Well as Recommendations for Reform*, 5 (Summer 2003), http://www.idtheftcenter.org/idaftermath.pdf. Terrorists might use all three types of ID theft. *See The Identify Theft Penalty Enhancement Act: Hearing on S.2541Before the Senate Judiciary Subcomm. on Technology, Terrorism and Government Information*, 107th Cong. (2002), (statement of Dennis M. Lorel, FBI Chief of the Terrorist Financial Review Group), *available at* http://www.fbi.gov/congress/congress02/idtheft.htm.

1999, one author described ID theft as the "cybercrime of the millennium,"[4] while others called it the fastest growing crime in America.[5] Given the fact that a millennium is an awfully long period of time coupled with our amazing ingenuity of finding novel methods of stealing from one another, the first description might prove to be an overstatement. There can be little doubt, however, that the second is not.

In terms of the number of victims, ID theft is indeed the fastest growing crime in America. A recent survey shows that in the last two years, almost twenty million Americans became new victims of ID theft—10.1 million in 2003 and another 9.3 million in 2004.[6] Another survey indicated that eighteen percent of Americans report themselves to be victims of ID theft.[7] In addition to survey data, the actual number of consumer ID theft complaints made to the Federal Trade Commission ("FTC") has steadily increased over the last three years to nearly 250,000 such complaints in 2004.[8]

One would imagine that this epidemic of ID theft would motivate the government—with the cooperation of the business world—to create some kind of "war on identity theft" in the same fashion as the war on drugs.[9] In fact, efforts by the federal

---

[4] *See generally* JOHN Q. NEWMAN, IDENTITY THEFT: THE CYBERCRIME OF THE MILLENNIUM, (Loompanics Unlimited, 1999); Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423 (Winter 2001).

[5] *See, e.g.*, IdentityTheft.org, Startling Facts about Identity Theft, (2005), http://www.identitytheft.org/startling_facts.htm; Sarah Scalet, *Five Ways to Stop Identity Theft*, CSO ONLINE, (March 2004), http://www.csoonline.com/read/030104/idtheft_2286.htm.

[6] *See* Javelin Strategy and Research, 2005 Identity Fraud Survey Report (Jan. 2005). A complementary overview of the survey can be requested from http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.php. The 2003 figure is based on a reevaluation of the 9.91 million figure contained in the 2003 Federal Trade Commission (FTC) survey report: SYNOVATE &FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT 7 (Sept. 2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

[7] *See* The Experian-Gallup Organization, Personal Credit Index (2005), http://www.personalcreditindex.com/PCI_Site/Gallup_Archive_Content.aspx?id=6.

[8] CONSUMER SENTINEL, NATIONAL AND STATE TRENDS IN FRAUD & IDENTITY THEFT: JANUARY –DECEMBER 2004 10 (Feb. 1, 2005), http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf (noting that the number of consumer ID theft complaints for the last three years were: 2002—161,896; 2003—215,093; and 2004—246,570).

[9] *See, e.g.*, Frontline, Thirty Years of America's Drug War, http://www.pbs.org/wgbh/pages/frontline/shows/drugs/cron/ (last visited Feb. 1,

government, however heralded in the media,[10] have been largely cosmetic at best, and have exacerbated the ID theft problem, at worst. In addition, Big Business continues to contribute to ID theft and has even found ways to profit from it.[11] A conspiracy theorist could easily conclude that business and government have worked together to place the burden of this growing blight on individual ID theft victims and the public in general.[12] The absence of meaningful institutional commitments to eliminate ID theft indicates that it is unlikely ID theft will substantially decrease any time soon. Unfortunately, it is much more probable that ID theft will continue to increase steadily for the foreseeable future.

With so much visible public concern over the issue of ID theft, the question is why society allows this problem to fester. This article will help the reader to understand the answer to that question by examining the environmental conditions that promote ID theft. It will discuss how ID theft is accomplished, the effects of ID theft, factors that contribute to ID theft and proposals for attacking the problem.

How the ID Thief Might Steal Your Identity

ID theft can be accomplished in a myriad of ways.[13] However,

---

2006) (suggesting that had such a war on ID theft been declared, it would likely have been even less successful than the war on drugs).

[10] *See, e.g.*, Davie McGuire, *Bush Signs New Identity Theft Bill*, WASH. POST, July 15, 2004, *available at* www.washingtonpost.com/wp-dyn/articles/A51595-2004Jul15.html (describing the Identity Theft Penalty Enhancement Act as a "tough new" law due to increased sentences for convicted ID thieves). *See also* The White House, President Bush Signs Identity Theft Penalty Enhancement Act (July 15, 2004), http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html (suggesting that the new legislation "will dramatically strengthen the fight against identify theft and fraud").

[11] *See* Joe Light, *Businesses See Profit in Fear of Identity Theft*, BOSTON GLOBE, Aug. 17, 2005, *available at* http://www.boston.com/business/articles/2005/08/17/businesses_see_profits_in_fear_of_identity_theft/.

[12] *See* George May, *Stop Thief!—Are Credit Bureaus and Creditors "Silent" Co-Conspirators To Identity Theft?*, 5 No. 3 J. TEX. CONSUMER L. 74 (Spring 2002), *available at* http://www.jtexconsumerlaw.com/TCL_WebSpring2002/pdf_files/IdentityV5N3.pdf.

[13] New ingenious methods of stealing personal data are developed every day. *See, e.g.*, Robert Vamois, *USB Devices Offer and Old-School Way to Steal Data*, CD NET (Aug. 12, 2005), http://reviews.cnet.com/4520-3513_7-6296529-1.html?tag=nl.e501.

there are two general approaches: the tried and true traditional methods, and newer online methods. The traditional methods include: 1) the acquisition of lost or stolen wallets, checkbooks or credit cards; 2) theft by friends, relatives or acquaintances; 3) information accessed as part of an offline transaction; 4) corrupt employees misappropriating company data; 5) stolen paper mail or fraudulent address changes; and, the perennial favorite, 6) rummaging through garbage, or "dumpster diving."[14] The newer online methods to steal an individual's identity can be accomplished through: 1) computer spyware; 2) accessing information as part of an online transaction; 3) creating computer viruses and hacking; and 4) sending "spoof"[15] emails posing as legitimate businesses, or "phishing".[16] A recent survey reports that of those ID theft victims who knew how their information was stolen, 68.2% reported the information was stolen using offline methods,[17] whereas the percentage for online methods

---

[14] Javelin, *supra* note 6, at 7.

[15] A tutorial on "spoof" emails provided by eBay is available at http://pages.ebay.com/education/spooftutorial (last visited Mar. 6, 2006). eBay has been used frequently in such fraudulent emails.

[16] Most readers who use email are familiar with this ever increasing problem. This "phishing" explosion has been the subject of a great deal of literature. *See, e.g.*, Robert Louis B. Stevenson, *Plugging the "Phishing" Hole: Legislation Versus Technology*, 2005 DUKE L. AND TECH. REV. 6, *available at* http://www.crime-research.org/analytics/phishing_duke; Federal Trade Commission, *How Not to Get Hooked by a 'Phishing' Scam*, FTC FOR THE CONSUMER, June 2005, http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm. For additional information, see Anti-Phishing Working Group, http://www.antiphishing.org, (last visited Jan. 26, 2006). For a good tutorial on spoof emails and fake web pages, see Mat Bright, *Spoof Email Phishing Scams and Fake Web Pages or Cites*, PHISHING SCAMS TUTORIAL PART 1 (Feb. 23, 2004), http://www.millersmiles.co.uk/identitytheft/gonephishing.htm. Screen captures of spoof emails are available for viewing at MillerSmiles (2005), http://www.millersmiles.co.uk/identitytheft/spoof-email-and-spoof-web-page-library.htm.

[17] The figures for offline ID theft methods were as follows:

Lost or stolen wallets, checkbooks or credit cards: 28.8%

Information stolen by friends, relatives or acquaintances: 11.4%

Information accessed as part of an offline transaction: 8.69%

Information stolen by corrupt employees who had access: 8.7%

Stolen mail or fraudulent changes of address: 8.0%

Information taken from garbage: 2.6%

was only 11.6%.[18] Although this data indicates the chances of ID theft via traditional methods is far more likely, research shows that Americans fear the Internet as a source of ID theft more than any other source.[19]

There is good reason for this fear. Recently, there have been numerous media reports of major personal information thefts—information that can be used to commit ID theft. In February 2005, data broker Choicepoint reported the theft of 145,000 individuals' personal information from its system.[20] By October of the same year, the personal information of over 50 million people had been stolen,[21] the vast majority of which was accomplished though the Internet.[22] Many types of institutions have been subject to such thefts. For example, Lexis-Nexis, banks, health providers, many universities and even the Air Force have reported such thefts.[23] Undoubtedly, the

---

See Javelin, *supra* note 6, at 7. The complementary Javelin report used does not indicate the percentage of total victims that knew how their information was stolen. The 2003 FTC report states that fifty-one percent of those in the study who knew how their information was stolen. *See* Synovate, *supra* note 6, at 30.

[18] The figures for online ID theft methods were as follows:

Computer spyware: 5.2%

Information accessed as part of an online transaction: 2.51%

Computer viruses or hackers: 2.2%

Emails sent by criminals posing as legitimate business: 1.7%

See Javelin, *supra* note 6, at 7.

[19] Sixty-two percent of survey respondents are somewhat or very fearful that their information will be stolen over the Internet. *See* Experian-Gallup, *supra* note 7. The next highest area of concern was the respondents' own mailbox, at fifty-five percent. *Id.*

[20] *See* Matt Hines, *Choice Point Data Theft Widens to 145,000*, CNET TECH NEWS FIRST, Feb. 18, 2005, http://news.com.com/ChoicePoint+data+theft+widens+to+145%2C000+people/2100-1029_3-5582144.html.

[21] *See* Privacy Rights Clearinghouse, A Chronology of Data Breaches Reported Since the ChoicePoint Incident, (Apr. 20, 2005), http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited October 2, 2005). The actual number of people affected may be less as the personal information of some individuals may have been contained in more than one repository.

[22] *Id.*

[23] *Id. See also* Roy Mark, Hacker Hits Air Force Database (Aug. 22, 2005), http://www.internetnews.com/security/article.php/3529046 The largest theft involved forty million credit card numbers from CardSystems Solutions, Inc., a

fraudulent use of even a small percentage of this personal information would result in a dramatic increase in the Internet as a source of ID theft information.[24]

In addition to providing an ever-increasing source of the personal identifiers used to commit ID theft, the Internet is an important tool ID thieves use to evaluate potential victims. For example, ID thieves prefer potential victims with either good credit or with no credit record at all. The latter has caused a substantial increase in teen and college student victims.[25]

The massive amount of personal information available on the Internet for free or a small charge allows the ID thief to cull out potential victims with the best characteristics.[26] As the Internet continues to grow as the largest depository of information in the world, it will certainly play an increasingly significant part in the ID theft crisis.

The Effects of ID Theft

The effects of ID theft on businesses and individuals are enormous. The total cost of ID theft was over $50 billion in each of the last two years.[27] In 2004, the mean cost per ID theft victim was

---

credit card data processing company, stolen by using a computer worm. Dana Blackenhorn, Identity Theft Turning Point? (June 28, 2005), http://www.corante.com/mooreslore/archives/2005/06/28/identity_theft_turning_point.php.

[24] As of August 2005, the ChoicePoint break-in data was used in "about 750 identity theft scams." Rita-Lynn Sanders, *Administrators Hold Key to Lock Down iSeries Security*, ISERIES NETWORK, Aug. 8, 2005, http://www.iseriesnetwork.com/content/f3/index.cfm?fuseaction=news.viewArticle&webID=1001&newsID=5021&issueID=5352&articleID=51367. One of the first ID theft prosecutions resulting from use of the ChoicePoint data involved sixteen victims and the theft of over four million dollars. *See* TechNews, *Identity Theft Case Filed in Los Angeles*, TECH. NEWS DAILY, Sept. 1, 2005, http://www.technologynewsdaily.com/node/1369.

[25] *See, e.g.*, NewsHour Extra, *Emerging Identity Theft Market Targets Teens as Newest Niche*, PBS ONLINE, Sept. 7, 2005, http://www.pbs.org/newshour/extra/features/july-dec05/idtheft_8-29.html; Kaniqua S. Daniel, *Identity Theft Greets Incoming Freshmen*, THE OAKLAND PRESS, Sept. 6, 2005, *available at* http://www.theoaklandpress.com/stories/090605/loc_2005090623.shtml; OhioNewsNow, *Kent State Warns of Identity Theft*, ONN NEWS, Sept. 12, 2005, http://www.onnnews.com/Global/story.asp?S=3832497&nav=LQlCeNEA..

[26] *See* May, supra note 12, at 73.

[27] $51.4 Billion in 2003 and $52.6 Billion in 2004. Javelin, *supra* note 6, at 5.

$5,686, and the mean out-of-pocket cost per victim was $652.[28] In the last year alone, the aggregate amount paid out-of-pocket by ID theft victims to address their individual theft problems exceeded $6 billion.[29]

Identity theft also creates indirect monetary costs such as the money paid by consumers to insure against such thefts.[30] A 2004 study estimates that ID theft insurance is already a $2.5 billion dollar industry.[31]

Moreover, ID theft has a significant impact on the economy in general. For example, fear of ID theft inhibits the full utilization of the Internet.[32] A 2000 FTC report cites a study which estimated $18 billion in lost Internet sales by 2002, due to consumer fears of Internet privacy.[33] The cost associated with investigating, arresting, prosecuting and imprisoning ID thieves is yet another blow to the economy.

ID theft imposes additional costs that are not readily measurable in monetary terms. For example, the time wasted by ID theft victims and businesses to address ID thefts is astronomical. In the last two years, identity theft victims spent nearly 600 million hours resolving ID theft problems not counting the time spent by businesses.[34] Other non-monetary costs to individual ID theft victims

---

[28] *Id.* These figures represent increases over 2003 where the mean costs were $5,072 and $536 respectively. *Id.*

[29] *Id.*

[30] *See* Light, *supra* note 11. *See also* Robert Gellman, Consumers and Costs—How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete 25-28 (Mar. 2002), https://www.epic.org/reports/dmfprivacy.pdf.

[31] CALPIRG Educational Fund, *Financial Privacy in the States—How Consumers Benefit from Personal Information Safeguards,* 27 (Feb. 2004), http://calpirg.org/reports/financialprivacy04.pdf.

[32] *See* Gellman, *supra* note 30, at 16. Online banking has been hit particularly hard. OUT-LAW News, *Online banking growth flattens due to security fears,* OUT-LAW, July 9, 2005, http://www.out-law.com/page-6098.

[33] FTC, Privacy Online: Fair Information Practices in the Electronic Marketplace 2 (2000),

http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[34] *Id.* This figure is based on the 10.1 million victims in 2003 multiplied by the mean resolution time of 33 hours for that year plus the 9.3 million 2004 victims, multiplied by the 28 hour mean resolution time for that year—a total of 593.7 million hours. *Id.* Slowly but surely, identity theft is starting to create a drag on the

can be even more significant. ID theft can likewise be emotionally devastating to its victims,[35] while at the same time damaging or ruining their credit.[36] During the period when the ID theft victim's credit is damaged, he or she may not be able to engage in such normal activities as financing a car, qualifying for a mortgage, renting an apartment or even finding a job.[37]

Clearly, the effects of ID theft on individuals, businesses and society are horrendous. Yet this pox on our house problem continues to grow virtually unabated. How could this have happened? Unfortunately, this cancer is allowed to grow more by choice than by accident. The next section examines the forces that contribute to the rise in ID theft and inhibit its elimination.

Forces That Contribute to ID Theft

Certainly, there are practical factors which might encourage ID thieves and thereby contribute to the rise in ID theft. It is easier, more profitable, requires no contact with the victim, is less likely to result in arrest and conviction and bears a lower penalty than many other criminal options.[38] These considerations are not the issue here. The real issue is the economic environmental factors that promote ID theft and inhibit its elimination, including the availability of personal data in the information age, the ability of businesses to pass the cost of ID theft on to the general public, the conduct of lenders and credit bureaus, the use of social security numbers as a universal identifier

---

economy.

[35] *See* Identity Theft Resource Center, Identity Theft—The Aftermath 2003: A Comprehensive Study—to Understand the impact of Identity Theft on Known Victims as Well as Recommendations for Reform 35-39 (Summer 2003), https://www.idtheftcenter.org/idaftermath.pdf.

[36] *See* Identity Theft Resource Center, How Can You Decrease Your Risk of Becoming a Victim of Identity Theft? (January, 2003), http://www.idtheftcenter.org/html/prevention_tips.htm.

[37] *See* Gellman, *supra* note 30, at 5.

[38] *See, e.g.*, Nadine Wimmer, *Identity Theft Prevention*, WHITE CANNON SOFTWARE, Feb. 2, 2004, http://www.whitecanyon.com/identity-theft-prevention-ksl-02-2004.php (stating that "[p]olice make arrests in violent crime more than 50 in 100 cases. They make arrests in identity theft in about 1 in 700 cases"); BCS Alliance, Identity Theft, http://www.bcsalliance.com/identitytheft.html (last visited Feb. 4, 2006) (stating that if you commit identity theft, your odds of ever being caught and prosecuted are about 1 in 750). *See also*, Sara Berg, Identity Theft: Business Victimization, 2 (Winter 2003), http://www.sparsa.org/research/IDTheft.pdf.

and counterproductive action by the federal government. These factors are interconnected, but will be examined separately below.

The Information Age

We are told at every turn that we live in "The Information Age." However defined, we live in a time when the collection, retention, purchase and sale of information is in itself a major economic activity and a facilitator for virtually all other economic activity.

Personal information is the "lifeblood" of ID theft,[39] and a conflict has developed between individual privacy and free accessibility. Business interests embrace one side of this debate. Privacy advocates, consumer advocates and ID theft victims take the other.[40] Business interests maintain that the collection, retention, purchase and sale of personal data should proceed unimpeded and that whatever problems may exist are best addressed by business self-regulation rather than governmental interference.[41] Business interests argue that the economy will benefit from this free flow of personal information,[42] and that unhindered access to such information will even contribute to the reduction of ID theft.[43]

Privacy advocates, on the other hand, argue that the

---

[39] Emily Finch, *What a Tangled Web We Weave: Identity Theft and the Internet*, in DOT.CONS: CRIME, DEVIANCE, AND IDENTITY ON THE INTERNET 86, 94 (Y. Jewkes ed., 2003), *available at* http://www.popcenter.org/Problems/Supplemental_Material/identity_theft/Finch_2003.pdf.

[40] *See* FTC Public Workshop: Information Flows: The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information, (June 18, 2003) (hereinafter "Information Flows Workshop"), http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.html

[41] *See id.*

[42] *See id.* at 2 (testimony of Charles D. Morgan, Chief Executive Officer of Acxiom Corporation, quoting Federal Reserve Board Chairman, Alan Greenspan, as follows:

> The flow of information on the characteristics of customers, both businesses and individuals, and changes in information technology in recent years, have improved the efficiency, innovativeness and competitiveness of our markets. This information has enabled producers and marketers to fine-tune production schedules to the ever greater demands of our consuming public for diversity and individuality of products and services).

[43] *See id.* at 6 (testimony of Laura DeSoto, Senior Vice President of Credit Services for Experian, one of the nation's three major credit bureaus).

unrestrained "free flow of information" is the primary cause of the rise in ID theft,[44] and is not the boon that business believes it to be.[45] They contend that the business models that support free access to personal data are incorrect and that the unbridled availability of personal consumer information leads to many societal costs, including increased ID theft.[46] They also argue that privacy and profitability can go hand in hand.[47] Certainly, ID theft victims support the position that personal information should be better protected and access to such information more restricted.[48] One thing is certain: whatever other effects might result, if the personal information necessary to commit ID theft was not readily available, thefts would necessarily decrease.

While it might have been true to some extent in past administrations, there is little doubt that during the George W. Bush Administration the voice of business is heard louder in Washington than that of consumers even if presented at the same volume.[49] Hence, for the time being business has won this debate and personal information remains available essentially unregulated. For less than

---

[44] *See* David Algoso et al., *Financial Privacy in the States—How Consumers Benefit from Person Information Safeguards*, CALPIRG 11 (Feb., 2004), http://calpirg.org/reports/financialprivacy04.pdf:

> Unrestrained information flow can increase a company's profits, but makes a customer's personal information accessible to more parties. This wide availability has made identity theft easier, and the electronic storage of sensitive information in an increasing number of places makes thieves difficult to track down.

[45] *See* Information Flows Workshop, *supra* note 40, at 3-5 (noting written comments of Beth Givens, Director of the Privacy Rights Clearing House submitted as an addendum to her testimony).

[46] *See* Gellman, *supra* note 30.

[47] *See* CALPIRG, *supra* note 31, at 29-30.

[48] *See* IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT—THE AFTERMATH 2003: A COMPREHENSIVE STUDY TO UNDERSTAND THE IMPACT OF IDENTITY THEFT ON KNOWN VICTIMS 39-43 (Summer 2003), http://www.idtheftcenter.org/idaftermath.pdf. *See also*, Janine Benner, *Nowhere to Turn—Victims Speak Out on Identity Theft*, CALPIRG (May 2000), http://calpirg.org/CA.asp?id2=3683&id3=CA&.

[49] *See, e.g.*, Testimony of Beth Givens, *supra* note 45, at 7 (complaining of FTC bias in that the ratio of business participants to privacy advocates at the workshop was approximately six to one). *See also* Elizabeth Drew, *Selling Washington*, NEW YORK REVIEW OF BOOKS, June 23, 2005, http://www.nybooks.com/articles/18075.

fifty dollars, information brokers will sell anyone all the personal information necessary to commit ID theft.[50] As long as we as a society continue to choose the free flow of personal information over the protection of privacy, ID theft will remain a significant part of our lives.

Passing the Costs of ID Theft On To Consumers

As noted before, one survey reported the costs of ID theft in 2004 to be $52.6 billion, with the out-of-pocket costs to individual victims constituting only $6 billion of that amount.[51] This means that business losses from ID theft were over $46 billion in just the last year. If these amounts represented "true" losses, major creditors and other businesses that "suffered" these losses would be screaming bloody murder to have an end put to ID theft. Instead, it is consumer and privacy groups that are pushing for ID theft prevention. Why is that? The answer is simple. Consumers rather than businesses actually suffer these losses.

Consumers shoulder these losses because businesses can pass the cost of ID theft on to them.[52]

Consumers bear the brunt of financial losses incurred by corporate identity thefts through higher costs for products and services. The costs of check fraud-losses, legal fees, increased insurance premiums, and higher banking costs are often if not always passed on to the consumer in the form of higher interest rates and other financial institution fees.[53]

Instead of extending credit cautiously in light of the high incidence of ID theft, there has been a virtual explosion of credit offers.[54] This ability to pass on the costs of ID theft contributes to the

---

[50] *See, e.g.*, Background Searcher, The Truth Is Here, http://www.backgroundsearcher.us (last visited Mar. 2, 2006); Public Records Search, Access Almost Any Public Record, http://www.records-search.net (last visited Mar. 2, 2006).

[51] *See* Javelin, *supra* note 6, at 1.

[52] *See* BCS Alliance, Identity Theft, http://www.bcsalliance.com/identitytheft.html (last visited Jan. 24, 2006).

[53] Information Security Newsletter, "Corporate" Identity Theft: A New Twist (Michigan State University, Theft Partnerships for Prevention, School of Criminal Justice), Jan. 15, 2002, http://www.cj.msu.edu/%7Eoutreach/identity/news4.html. *See also*, Sara Berg, *Identity Theft: Business Victimization*, ENTERPRISE SECURITY 6 (Winter 2003), *available at* http://www.sparsa.org/research/IDTheft.pdf.

[54] *See* Bob Sullivan, *Deluged with Credit Card Mail? Help is Coming*,

credit offerings we annoyingly find in our mailboxes nearly every day.

The credit card industry is a prime example of this situation. Credit card fraud associated with the fraudulent use of existing credit card accounts or the creation of new credit card accounts is the most common type of ID theft.[55] Yet, credit card offers abound and credit is all too often granted with inadequate proof of identity.[56] Competition in the credit card industry is fierce. Lenders believe they cannot reduce their competitive zeal simply because they engage in a risky business. To offset these risks—one of which is ID theft—they simply raise their interest rates and fees.[57] By paying these higher interest rates and fees, you and I, rather than the credit card companies, pay the cost of ID theft.

Many of the proposals for reducing ID theft require lenders to be more careful when extending credit.[58] As long as creditors can pass the bulk of ID theft cost on to the public, they have little incentive to advocate enacting such proposals into law.[59] For them, ID theft is simply a cost of doing business that can be passed on without decreasing profitability. Until the costs of ID theft are so high they cannot be passed on—until the public rejects credit cards

---

MSNBC, Aug. 8, 2005, http://www.msnbc.msn.com/id/8827007/ (citing one survey that estimated that 1.4 billion credit card solicitations were sent out in the first quarter of 2005).

55 *See* SYNOVATE, FEDERAL TRADE COMMISSION—IDENTITY THEFT SURVEY REPORT 10 (Sept. 2003), http://www.ftc.gov/os/2003/09/synovatereport.pdf.

56 *See* Liz Pulliam Weston, *Blame Lenders, not Thieves, for Identity Theft*, MSN MONEY, March 2005, http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P48173.asp.

57 Ryan Kim, *Why Credit Card Rates are Rising—Banks Use Lots of Reasons for Increasing Interest*, SFGATE, July 28, 2005, http://sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2005/07/28/BUG8RDUGKV1.DTL&type=business.

58 *See, e.g.*, PIRGIM, Michigan Detectives: Identity Theft on the Rise—New Laws, Resources Needed to Deter Identity Theft, Feb. 4, 2004, http://pirgim.org/MI.asp?id2=12099&id3=MI& (stating that the primary recommendation was to require credit card companies and other credit grantors to tighten security before granting credit). The full PIRGIM report is available at http://pirgim.org/reports/policingprivacy04.pdf.

59 *See* BCS Alliance.com, *supra* note 52:

> The problem with identity theft is that much of it could easily be prevented if Congress would pass laws requiring lenders and sellers to thoroughly verify each and every credit application, but if the did so, it would cost the banking industry billions, so they don't require them to.

because the interest rates and fees are too high—ID theft will continue to prosper. That point in time, should it ever come, lies beyond the immediate horizon.

Lenders and Credit Bureaus

Credit reporting agencies ("CRAs"), commonly referred to as credit bureaus, were created to assist lenders in assessing the credit worthiness of potential borrowers.[60] Over the years, both the availability of consumer credit and the personal information maintained by CRAs has risen exponentially.[61] The development of these industries, lenders and CRAs[62] have facilitated the rise in ID theft.[63]

Some place the primary blame on lenders for extending credit "with only a cursory validation that the person requesting credit is truly who he or she purports to be."[64] Others include CRAs as a principle culprit.[65] Certainly, there is hyperbole in such statements as

---

[60] For a history of the credit reporting industry in America, see Robert M. Hunt, *A Century of Credit Reporting in America,* (Fed. Reserve Bank of Phila., Working Paper No. 05-13, 2005), *available at* http://www.phil.frb.org/files/wps/2005/wp05-13.pdf. *See also FTC Prepared Statement on the Fair Credit Reporting Act Before the Fin. Inst. And Consumer Credit Subcomm. of the House Fin. Serv. Comm.* (2003), *available at* http://www.ftc.gov/os/2003/06/030604fcratestimony.pdf [hereinafter PREPARED STATEMENT].

[61] *See* Hunt, *supra* note 60, at 2:

> In 2002, Americans held more than 1.5 billion credit cards, used them to spend $1.6 trillion, and maintained balances in excess of $750 billion. Information provided by credit bureaus us an important ingredient in the vast expansion of unsecured consumer credit in the U.S. over the last century.

[62] *Id.* at 16-17. Today in America there are three major credit bureaus: Equifax, Experian and TransUnion. There are less than 1,000 smaller credit bureaus and a number of specialty credit bureaus dealing with such issues as landlord-tenant and employment. *Id.* at 16-17. Almost all of these smaller or specialty credit bureaus get their information from the big three. *Id.* at 16-17.

[63] *See* Weston, *supra* note 56; NEWMAN, *supra* note 4, at 11-15 (discussing credit bureaus as "Partners in Identity Theft").

[64] Mark Peters, *Proposal to Reduce Identity Theft with Personal Identification Numbers*, EPINIONS, Aug. 8, 2003, http://www.epinions.com/content_3442778244. *See also* Weston, *supra* note 57; Mike Lee & Brian Hitchen, *Identity Theft—The Real Cause,* IT OBSERVER, May 24, 2004, http://www.ebcvg.com/articles.php?id=217.

[65] *See* NEWMAN, *supra* note 4, at 11-15.

it is the ID thieves that actually commit the crimes. It is true, however, that the individual behavior of creditors and CRAs, as well as the interrelationship of these two forces, facilitate ID theft. Even assuming their intentions are entirely innocent, creditors and CRAs facilitate ID theft both before and after the fact.[66]

In addition to contributing to ID theft by sending out billions of unsolicited credit offers[67] and by using careless credit granting procedures, creditors also contribute to ID theft by ignoring fraud alerts on consumers' credit reports and failing to cooperate with law enforcement attempts to investigate the crime.[68] The Fair and Accurate Credit Transactions Act of 2003 ("FACTA")[69] modified the Fair Credit Reporting Act ("FCRA"),[70] which regulates CRAs, by adding new sections and changing some of the existing provisions.[71] One new provision allows identity theft victims to notify one CRA and have all three major CRAs put a "fraud alert" on their credit

---

[66] *See* Benner, *supra* note 48, *Nowhere to Turn—Victims Speak Out on Identity Theft*, CALPIRG 10 (May 2000), http://calpirg.org/CA.asp?id2=3683&id3=CA&:

> Yet, much more needs to be done to stop identity theft. In particular, legislation must be enacted to require creditors and credit bureaus to improve their credit-granting and complaint-handling practices. Further, easy access to the bits of information that comprise a consumer's financial identity must be curtailed. Sloppy credit-granting practices by banks, department stores, phone services, and other creditors make the crime all too easy to commit. Once the crime has occurred, creditor and credit bureau practices help perpetuate the problem by subjecting victims to a nightmarish system of clearing their names, making victims into repeat victims, or both.

[67] *See* Bob Sullivan, *Deluged with Credit Card Mail? Help is Coming*, MSNBC, Aug. 8, 2005, http://www.msnbc.msn.com/id/8827007/ (estimating that 1.4 billion credit card solicitations were sent out in the first quarter of 2005).

[68] *See* Weston, supra note 56.

[69] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159 (2003).

[70] 15 U.S.C. § 1681 *et seq.*

[71] *See* Privacy Rights Clearinghouse, FACTA, The Fair and Accurate Credit Transactions Act: Consumers Win Some and Lose Some (2005), http://www.privacyrights.org/fs/fs6a-facta.htm#1; NCLC, Analysis of the Fair and Accurate Credit Transactions Act of 2003, http://www.nclc.org/initiatives/facta/contents/nclc_analysis_content.html#1#1 (last visited Feb. 4, 2006).

reports.[72] Linda Foley, Executive Director of the Identity Theft Resource Center, contends that creditors are ignoring these fraud alerts because they claim it is too expensive to contact consumers to verify credit applications.[73] Creditors fail to cooperate with law enforcement in a number of ways. A study of law enforcement's response to ID theft reports investigators as saying they regularly encountered lenders who failed to return police calls, refused to provide copies of credit applications and even ignored some search warrants.[74]

There are several other more insidious ways in which creditors might contribute to ID theft. One is to knowingly report fraudulent information to the CRAs as genuine.[75] Creditors are aware that negative information on a credit report, even if inaccurate, might well force the innocent party to pay the fraudulent debt.[76] Another disreputable practice is for creditors to sell ID theft debts to debt collectors. A provision of FACTA prohibits such sales,[77] but consumers have no private right to sue for a violation under this provision, and there is no evidence that creditors will abide by it. Whether through greed, negligence or willful misconduct, creditors continue to facilitate ID theft. Until the losses from such behavior exceed the potential profits, creditors will remain one of the principal contributors to ID theft.

CRAs have been referred to as "partners in identity theft."[78] There are three major CRAs in the United States: Experian, Equifax

---

[72] 15 U.S.C. § 1681a(q)(3).

[73] *See* Weston, *supra* note 56.

[74] JENNETTE GAYER, CALPIRG EDUCATIONAL FUND, POLICING PRIVACY: LAW ENFORCEMENT'S RESPONSE TO IDENTITY THEFT 9-10 (2003), http://calpirg.org/reports/policingprivacy2003.pdf.

[75] Creditors who provide information to credit bureaus are known as "furnishers." *See* 15 U.S.C. § 1681s-2(a)(6). Prior to the 1996 amendments to the FCRA, furnishers could not be sued under the act by consumers for providing inaccurate information to credit bureaus. Even after the changes, furnisher litigation is still uncommon. Unscrupulous creditors are willing to take the chance the innocent "debtor" will pay to clean up their credit rather than sue.

[76] *See* Sullivan v. Equifax, Inc., No. CIV. A. 01-4336, 2002 WL 799856, at *3-4 (E.D. Pa. Apr. 19, 2002) (referencing *Rivera v. Bank One*, 145 F.R.D. 614, 622-23 (1993); *Matter of Sommersdorf*, 139 B.R. 700, 701 (Bankr. S.D. Ohio 1991)).

[77] 15 U.S.C. § 1681m(f).

[78] *See* NEWMAN, *supra* note 4. *See also* Hoar, *supra* note 4.

and TransUnion.[79] Functionally, these three economic giants control the credit of all Americans as well as the citizens of many other countries.[80] If there is any "big three" left in this country, it is the CRAs, not the automobile companies.

The principal contribution of CRAs to ID theft is personal information. The amount of this information in the hands of CRAs is almost beyond comprehension. For example, in *Sarver v. Experian*,[81] the Court noted:

> The affidavit of David Browne, Experian's compliance manager, explains that the company gathers credit information originated by approximately 40,000 sources. The information is stored in a complex system of national databases, containing approximately 200 million names and addresses and some 2.6 billion trade lines, which include information about consumer accounts, judgments, etc. The company processes over 50 million updates to trade information each day.[82]

One would hope that with all this personal information, the accuracy of credit reports[83] would be a paramount consideration. Unfortunately, this is not the case. In credit reporting, speed, rather than accuracy, rules. A 2003 study[84] discovered that seventy-nine percent of all credit reports contain some type of error, and twenty-five percent contain such serious errors that those individuals could be denied credit.[85] By failing to put procedures in place to assure that the information in their files is accurate, and by continuing to

---

79 *See* Hunt, *supra* note 60. *See also* PREPARED STATEMENT, *supra* note 60.

80 *See* Hunt, *supra* note 60.

81 Sarver v. Experian, 390 F.3d 969, 972 (7th Cir. 2004).

82 *Id.*

83 For information about credit reports generally, see Privacy Rights Clearinghouse, How Private is My Credit Report?, (Nov. 1992, revised Feb. 2006), http://www.privacyrights.org/fs/fs6-crdt.htm#1.

84 U.S. PIRG, MISTAKES DO HAPPEN: A LOOK AT ERRORS IN CONSUMER CREDIT REPORTS (June 2004), *available at* http://uspirg.org/reports/MistakesDoHappen2004.pdf.

85 *Id.* at 4. *See also* Ray Martin, *Four out of Five Credit Reports Have Errors*, CBS NEWS, Oct. 13, 2004, http://www.cbsnews.com/stories/2004/10/12/earlyshow/contributors/raymartin/main648887.shtml.

circulate erroneous information—some of which is the result of identity theft—CRAs make it more difficult to both discover ID theft, as well as to enable victims to reestablish their credit.

CRAs are regulated under the FCRA.[86] The FCRA requires that third parties have a "permissible purpose" in order to obtain a credit report.[87] To comply with this requirement, CRAs must maintain reasonable procedures designed to assure that only those with proper purposes are permitted to acquire credit reports.[88] If these procedures are lax it is may be possible for ID thieves to obtain credit reports containing all the information necessary for the crime. More often the fault is not with lax procedures on the part of CRAs, but with dishonorable employees of CRA subscribers.[89] However, more rigorous procedures on the part of both subscribers and CRAs could diminish this problem.

More important, perhaps, is the exception to the "permissible purpose" rule permitted for affiliate sharing. Affiliate sharing allows the CRAs and their subscribers to share personal consumer information with related corporations.[90] An FCRA amendment[91] added by the FACTA limits an affiliate's use of consumer information unless the consumer is given an opportunity to opt-out of such use.[92] Few consumers choose to opt-out.[93] Affiliates in

---

[86] Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* (2005).

[87] Generally, reports may be provided for the purposes of making decisions involving credit, insurance, or employment. 15 U.S.C. § 1681b(a)(3) (2005). Consumer reporting agencies may also provide reports to persons who have a "legitimate business need" for the information. 15 U.S.C. § 1681b(a)(3)(F). The legitimate business need requires that the transaction be initiated by the consumer. 15 U.S.C. §1681b(a)(3)(F)(i).

[88] 15 U,S,C. § 1681e(a). *See also*, FTC Official Staff Commentary § 607 Item @G, item 2A. One large reporting agency, TRW, asserts it conducts both precautionary and investigative activities on the uses to which its clients put the reports. Klapper v. Shapiro, 154 Misc, 2d 459; 586 N.Y.S.2d 846 (1992).

[89] *See, e.g.*, Graves v. Tubb, 281 F. Supp. 2d 886 (N.D. Miss. 2003) (where an employee used his position to obtain credit information on his ex-wife and her new husband); Del Amora v. Metro Ford Sales and Service, Inc., 206 F. Supp. 2d 947 (N.D. Ill. 2002) (where an employee obtained credit information about his brother-in-law while his sister's divorce was pending).

[90] *See generally* Barbara M. Mishkin, *Fair Credit Reporting Act Amendments: Affiliate Sharing*, REED SMITH, Mar. 10, 2004, http://www.reedsmith.com/library/search_library.cfm?FaArea1=CustomWidgets.content_view_1&cit_id=3623.

[91] 15 U.S.C. § 1681s-3(a).

[92] *See* Mishkin, *supra* note 90.

possession of sensitive personal information obtained from the CRAs are often used as sources by ID thieves.[94]

It may well be that the greatest contribution CRAs have made to the rise of ID theft in this country is through the sale of "header" information.[95] Credit "header" information includes such personal identifying items as the consumer's name, address, telephone number, date of birth and social security number.[96] It does not include credit history items. Starting in the 1990s, the Federal Trade Commission ("FTC"), which is charged with regulating CRAs, held that "header" information could be sold outside the restrictions of the FCRA.[97] Given the green light, the CRAs—each with hundreds of millions of personal information files—began selling this information to data brokers, marketing firms, financial institutions and anyone else willing to pay for it. This information rests in the computers of those who purchased it, ready to be stolen or purchased by ID thieves.

In 1999, Congress passed the Gramm-Leach-Bliley Act ("GLBA"),[98] which contains a number of provisions designed to protect the privacy of nonpublic personal information at financial and financial-related institutions.[99] Pursuant to the GLBA, the FTC formulated a regulation which would restrict CRAs' sale of "header"

---

[93] Privacy advocates, consumer advocates and ID theft victims argue that an opt-in system for the use of information by affiliates would substantially reduce ID theft. Businesses, of course, prefer opt-out. For a discussion of the two systems see Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV. 1457, 1494-1501 (2001) (discussing the relative merits of opt-in and opt-out systems to sensitive personal information collected by commercial entities), *available at* http://www.ag.state.mn.us/consumer/PDF/BigBrother.pdf.

[94] The data brokers and financial institutions that have been subject to data breaches are often affiliates of CRAs.

[95] *See* Jeanne Sahadi, *Your Identity for Sale: From Credit Bureaus to Grocers to Unscrupulous Brokers, There's a Healthy Trade in Your Good Name*, CNN MONEY, May 9, 2005,http://money.cnn.com/2005/05/09/pf/security_info_profit/.

[96] Privacy Rights Clearing House, Federal Reserve Board "Credit Header" Comments, Jan. 30, 1997, http://www.privacyrights.org/ar/fedres.htm.

[97] *See* USPIRG, Letter Endorsing Nelson Markey Proposals Regulating Information Brokers 1 (Mar. 8, 2005), http://www.pirg.org/consumer/pdfs/pirgendorsesnelsonmarkey.pdf.

[98] Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.* (2000).

[99] *See* 15 U.S.C. §§ 6801-6809.

information.[100] TransUnion, one of the big three CRAs, sued the FTC to prevent the implementation of the new regulation.[101] In 2002, the Federal Court of Appeals held that the regulation was valid.[102] Hence, subsequent to 2002, CRAs are no longer allowed to sell "header" information without giving the consumer an opportunity to opt-out of such sales.[103] Although this may have somewhat reduced the sale of "header" information, it has far from eliminated the practice. As long as CRAs continue to collect, retain and sell our personal information, ID theft will continue to grow.

Social Security Numbers As Universal Personal Identifiers

Perhaps, the real key to ID theft[104] is the use of the social security number ("SSN") as a universal personal identifier.[105] None of the factors already considered—the profusion of personal information offered for sale by data brokers, the behavior of lenders in their zeal to sell their "products" and the huge deposits of personal information housed at CRAs—could have the impact on ID theft they do if our country stopped using SSNs as a universal personal identifier.[106] Support for this proposition is apparent by the fact that

---

[100] *See* TransUnion v. FTC, 295 F.3d 42, 50-51 (D.C. Cir. 2002).

[101] *Id.* at 50.

[102] *Id.* at 53.

[103] 15 U.S.C. § 6802(b).

[104] *See* Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, 4-6, *available at* http://stlr.stanford.edu/STLR/Articles/04_STLR_2/. *See also* Eileen Ambrose, *Secure Number is Key to Privacy*, Sun-Sentinal, Sept. 1, 2005, available at http://www.sun-sentinel.com/business/sns-yourmoney-0901security,0,5347909.story?coll=sfl-*yourmoney*. Social Security Administration, Identity Theft and Your Social Security Number (Feb. 2004), http://www.ssa.gov/pubs/10064.pdf.

[105] The social security number itself provides certain information about where you were born and your approximate age. Computer Professionals for Social Responsibility, Structure of Social Security Numbers, May 15, 2001, http://www.cpsr.org/prevsite/cpsr/privacy/ssn/ssn.structure.html.

[106] *See U.S. Public Interest Research Group Before the Subcommittee on Social Security of the H. Comm. On Ways and Means*, 108th Congress (June 15, 2004), http://waysandmeans.house.gov/hearings.asp?formmode=printfriendly&id=1648#_ednref1 (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group).

other modern countries that do not use a universal personal identifier such as our SSNs have a much lower incidence of ID theft.[107]

Proposals have been made for legislation protecting SSNs[108] and for a new, safer identity system.[109] The FACTA did give consumers a modicum of protection by permitting them to request that their SSNs be truncated when CRAs send out their credit reports (only the last four numbers sent).[110] With this exception, there are few laws regulating the use of SSNs by businesses. Unless we find some way of effectively protecting SSNs, or better yet, develop a personal identity system less amenable to abuse, ID theft will continue to plague our society.

Counterproductive Action By the Federal Government

As previously discussed, pressure to remedy ID theft comes from consumer groups, privacy advocates and victims. Big Business, on the other hand, is more interested in making sure it can pass the cost of ID theft on to the public and/or profit from it.[111] Given these circumstances, it would be unreasonable to expect the federal government, especially during the George W. Bush Administration, to attack the real causes of ID theft. True to those expectations, the federal government has done little to remedy the environmental factors that have contributed to the rise in ID theft. In fact, many of the laws passed during the Bush Administration have done more to

---

[107] *See* Liz Pulliam Weston, *What Europe Can Teach Us About Identity Theft*, MSN MONEY, June 2, 2005, http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P116528.asp.

[108] *Id. See also* The Orator, H.R. 220, The Identity Theft Prevention Act of 2005 (Proposed), http://www.theorator.com/bills109/hr220.html (last visited Mar. 1, 2006).

[109] *See, e.g.*, Lynn M. LoPucki, *Did Privacy Cause Identity Theft?*, 54 HASTINGS L.J. 1277 (2003), *available at* http://ssrn.com/abstract=386881 (The author proposes a pubic identity system arguing that because most identity impersonations take place in private transactions, the decrease in public identities over the last three decades coupled with the increase in privacy has provided an environment within which identity thieves can operate.)

[110] Fair Credit Reporting Act, 15 U.S.C. § 1681g(a) (2005).

[111] The most common way lenders profit from ID theft is by selling ID theft insurance. *See e.g.*, Laura Bruce, *Is Identity Theft Protection Worth the Money?*, BANKRATE, Aug. 4, 2004, http://www.bankrate.com/brm/news/advice/scams/20040804a1.asp; David Simons, *ID Theft Insurance Isn't Insurance*, FORBES, May 29, 2003, *available at* http://www.forbes.com/2003/05/29/cx_ds_0529simons.html.

exacerbate the problem than correct it.

One example is the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005.[112] In the usual legislative "doublespeak"[113] from this era, this bill neither prevents bankruptcy abuse nor protects consumers.[114] Some argue that this bill was bought and paid for by the banking, credit card and retail industries who "gave more than $56 million to political parties and candidates in the 2004 elections."[115] These businesses had been pressing for "bankruptcy reform" for several years, and it became one of their principal legislative targets after the increase in Congress's Republican majority in 2004.[116]

Essentially, this legislation, which took effect in October of 2005, makes it more difficult for individuals to declare bankruptcy without paying back some of their debts. It does not close loopholes for businesses or wealthy individuals that declare bankruptcy.[117] Democrats tried to pass amendments limiting the impact of the bill on the most vulnerable consumers[118] noting, for example, that about one-half of all bankruptcies are the result of medical problems.[119] All

---

[112] For a discussion of the provisions of the Bankruptcy Abuse and Consumer Protection Act, see Compact Library Publishers, Inc., Comprehensive Summary of the Bankruptcy Reform Act of 2005, http://ws5.com/bankruptcy (last updated May 17, 2005).

[113] Legislation passed during the George W. Bush Administration usually has names that are entirely inconsistent with their effects. *See* Molly Ivins, Under Clear Skies , Alternet, Sept. 19, 2003, http://www.alternet.org/story/16807/.

[114] *See, e.g.*, Editorial, San Francisco Chronicle, *How a Bad Bill Becomes Law*, SFGATE, Mar. 13, 2005, http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2005/03/13/EDGSMAPC9G1.DTL; Martin H. Bosworth, *Congress Passes Bankruptcy Reform Bill—Measure Rewards Financial Industry at Consumer's Expense*, CONSUMER AFFAIRS, Apr. 14, 2005, http://www.consumeraffairs.com/news04/2005/bankruptcy_act01.html.

[115] Kathleen Day, *Senate Passes Bill To Restrict Bankruptcy Credit Card Business Backed Measure to Collect More Debt*, WASH. POST, Mar. 11, 2005, *available at* http://www.washingtonpost.com/wp-dyn/articles/A24940-2005Mar10.html. *See also* Open Secrets, Tracking the Payback—Finance: Bankruptcy Reform (April 15, 2005), http://www.opensecrets.org/payback/issue.asp?issueid=BA3&CongNo=109.

[116] *See* Open Secrets, *supra* note 115.

[117] *See* Hunter, *The Bankruptcy Bill, Examined*, DAILY KOS, Mar. 6, 2005, http://www.dailykos.com/story/2005/3/6/63144/06015.

[118] *Id.*

[119] *See* David U. Himmelstein, et. al, *Marketwatch: Illness and Injury as*

of these amendments, including one specifically designed to protect individuals forced into bankruptcy as a result of ID theft, were defeated.[120] It is interesting to note that shortly after the Hurricane Katrina catastrophe, Democrats indicated an intention to introduce a bill to shield Katrina victims from the effects of the new bill.[121] As of this writing, it remains to be seen whether lenders will have the power to keep Congress from protecting these unfortunate individuals.

Part of the ID theft problem noted above results from lenders being able to pass the cost of ID theft on to the general public as well as their flooding the market with billions of credit card offers,[122] some of which end up in the hands of ID thieves. Rather than discouraging these behaviors, the bankruptcy "reform" bill will enable lenders to pass on even higher ID theft costs and will do nothing to restrain them from deluging us with never-ending waves of unsolicited credit card offers.

The FACTA,[123] mentioned above, is another example of counterproductive legislation. Although it is certainly true that the FACTA contains provisions that may benefit ID theft victims,[124] it is also a bill "written to protect the financial industry in this country."[125] The preemption provisions of the FACTA are prime examples of counterproductive federal action.

Contributors to Bankruptcy, HEALTHWATCH.ORG, Feb. 2, 2005, http://content.healthaffairs.org/cgi/content/full/hlthaff.w5.63/DC1. *See also and listen to* Patricia Neighmond, *Study Shows that Medical Bills Spur Slew of Personal Bankruptcies,* NPR, Feb. 2, 2005, http://www.npr.org/templates/story/story.php?storyId=4475013.

[120] *See* Hunter, *supra* note 117.

[121] *See, e.g.*, Martin Bosworth, *Congress May Modify Bankruptcy Reform that Penalizes Katrina Victims*, CONSUMERAFFAIRS.COM, Sept. 5, 2005, http://www.consumeraffairs.com/news04/2005/katrina_bankruptcy.html; Loren Steffy, *Law to Deal Second Blow to Victims of Hurricane*, HOUS. CHRON., Sept. 8, 2005, *available at* http://www.chron.com/cs/CDA/ssistory.mpl/business/3345871.

[122] One survey estimated that 1.4 billion credit card solicitations were sent out in the first quarter of 2005. Bob Sullivan, *Deluged with Credit Card Mail? Help is Coming*, MSNBC, Aug. 8, 2005, http://www.msnbc.msn.com/id/8827007/.

[123] Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159 117 Stat. 1952 (2003). *See also* National Consumer Law Center (NCLC), Analysis of the Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159 (2003), http://www.nclc.org/initiatives/facta/nclc_analysis.shtml.

[124] WEISMAN, *supra* note 1, at 169-182 (Pearson Education, Inc., 2005).

[125] *Id.* at 170.

When the FCRA was originally enacted in 1970, states were free to enact laws giving consumers more protections than those contained in the FCRA.[126] Amendments to the FCRA in 1996, with a few exceptions, established federal preemption preventing states from passing laws with greater restrictions on business than those contained in the FCRA.[127] These preemption provisions were set to expire in 2004.[128] The impetus for the FACTA was the desire of the financial industry to continue and expand the preemption of stronger state laws rather than any governmental mission to combat ID theft or protect its victims.[129] Since the bill had to be passed prior to the 2004 preemption expiration, the financial backers were willing to make some concessions to consumers in order to get the bill passed in time.[130]

Many commentators concede that whatever good the FACTA has delivered—such as one free credit report per year from each of the big three CRAs,[131] and the ability of ID theft victims to put fraud alerts on their credit reports[132]—was obtained at a high price.[133] For

---

[126] *See* Michael Epshteyn, *The Fair and Accurate Credit Transactions Act of 2003: Will Preemption of State Credit Reporting Laws Harm Consumers?*, 93 GEO. L.J. 1143, 1154 (2005).

[127] *Id.*

[128] *Id.*

[129] *Id.*

[130] *See* Weisman, *supra* note 1, at 169-70.

[131] 16 C.F.R. §§ 610.1-610.3.

[132] Fair Credit Reporting Act, 15 U.S.C. § 1681a(q)(3) (2005).

[133] *See* Epshteyn, *supra* note 126, at 1164-65:

> Congress took important and much-needed steps to strengthen the FCRA when it passed the Fair and Accurate Credit Transactions Act of 2003, and consumers should applaud the additional rights they have gained under this new legislation. These rights, however, have come at a high price, because states may no longer be able to effectively protect their citizens from unforeseen credit reporting dangers, and, as the growing practice of identity theft demonstrates, new threats may well lurk right around the corner. Implementing baseline national standards, while granting the states flexibility to legislate in this dynamic and unpredictable domain, would likely have been the best means of improving our credit system while simultaneously strengthening consumer protections. Congress's failure to adopt this approach may ultimately serve to undermine consumer privacy and financial security, although only time can tell whether the dire consequences of preemption forecasted by this Note will ever come to pass.

example, under the FACTA, consumers were given the new benefit of the ability to opt out of affiliate sharing, orwhich is the practice of CRAs sharing their personal information with related companies.[134] At the same time, the FACTA preempted any state laws that would further restrict affiliate sharing.[135] California had enacted a statute with stronger affiliate sharing restrictions than those contained in the FCRA.[136] In June 2005, in *American Bankers Association v. Gould*,[137] the Federal Court of Appeals struck down the California statute as preempted by the weaker FCRA.[138] Many of the states that have enacted or are considering laws addressing ID theft will find their efforts futile as a result of the FACTA preemptions.

With several of its new "protections" offered to ID theft victims, the FACTA compounds its preemption with the absence of a private right of action—the ability of individuals to sue if they have been injured by a violation of the FCRA. Without a capacity to sue for its breach, any new alleged "benefit" is functionally no benefit at all. For example, the FACTA requires that furnishers of information to CRAs maintain reasonable procedures to assure that they do not refurnish information to the CRAs once they are notified that the information is the result of ID theft.[139] This provision helps ID theft victims clear up their credit by preventing the erroneous information from reappearing on future credit reports. Therefore, if a credit card company has inadequate procedures in place and refurnishes ID theft information to the CRAs, the ID theft victim cannot sue for this breach[140] and states are preempted from enacting laws that would give ID theft victims the right to sue.[141]

Another piece of federal legislation that is at best cosmetic and could prove counterproductive is the Identity Theft Penalty

---

See also Privacy Rights Clearing House, *FACTA, The Fair and Accurate Credit Transactions Act: Consumers Win Some, Lose Some* (Apr. 2005), http://www.privacyrights.org/fs/fs6a-facta.htm; NCLC, *supra* note 123.

[134] 15 U.S.C. § 1681t(b)(1)(H). *See generally* Mishkin, *supra* note 90.

[135] 15 U.S.C. § 1681s-3.

[136] California Financial Information Privacy Act, CAL. FIN. CODE § 4050-60 (2004).

[137] Am. Bankers Ass'n v. Gould, 412 F.3d 1081, 1083 (9th Cir. 2005).

[138] *Id.* at 1087.

[139] Fair Credit Reporting Act, 15 U.S.C. § 1681s-2(a)(6)(A) (2005).

[140] 15 U.S.C. § 1623(a)(6)(B).

[141] 15 U.S.C § 1623(c).

Enhancement Act ("ITPEA").[142] Passed with much fanfare, the ITPEA increases the penalty for certain ID theft crimes by two years and terrorism using false IDs by five years.[143] Increasing the penalty for a particular crime will have the desired effect of reducing that crime only if the criminal is thinking logically[144] and the increased penalty makes the rewards of committing the crime unattractive. Since ID theft can be quite lucrative and the chance of getting caught is about seven hundred to one,[145] the ITPEA is unlikely to significantly deter ID theft; whatever kudos Congress and the President might have received for its passage. Moreover, the ITPEA might have a negative effect on the prevention of ID theft by lulling the public into a belief that the government is doing something about the problem. Consumers could thus be less inclined to demand real remedies and less vigilant regarding their personal data.

There are still other examples of federal government action that failed to address the real causes of the ID theft crisis and/or made the problem worse. Be that as it may, only a dramatic and immediate change can reverse the rising trend of ID theft.

Proposals for Changing the ID Theft Environment

Overview

In 2003, LexisNexis released a study of ID theft conducted in conjunction with the Economic Crime Institute of Utica College.[146]

---

[142] Pub. L. No. 105-318, 112 Stat. 3010 (1998).

[143] *See, e.g.*, David McGuire, *Bush Signs New Identity Theft Bill*, WASH. POST.COM, July 15, 2004, http://www.washingtonpost.com/wp-dyn/articles/A51595-2004Jul15.html; Press Release, The White House, President Bush Signs Identity Theft Penalty Enhancement Act (July 15, 2004), http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html.

[144] For example, the terrorists that flew their high-jacked planes into the World Trade Center and the Pentagon, several of whom were in the possession of false identifications, would hardly be deterred by the fact that their crime bore the possibility of five extra years in prison.

[145] *See Wimmer*, supra note 38 (noting that "[p]olice make arrests in violent crime more than 50 in 100 cases. They make arrests in identity theft in about 1 in 700 cases."); BCS Alliance, Identity Theft, http://www.bcsalliance.com/identitytheft.html (stating that ". . .if you commit identity theft, your odds of ever being caught and prosecuted are about 1 in 750") (last visited Feb. 4, 2006).

[146] DR. GARY R. GORDON & NORMAN A. WILCOX, JR., ECONOMIC CRIME INSTITUTE OF UTICA COLLEGE, IDENTITY FRAUD: A CRITICAL AND GLOBAL

Analyzing the ID theft problem, the study noted that: "Identity fraud has become a national and global problem. Once a problem has risen to that level, the government must take a central role in providing the leadership to help solve it."[147] Hence, the study's first recommendation was "a commitment from the highest levels of federal government to lead and fund a national strategy to combat the identity fraud problem."[148] This recommendation would require the federal government to sever its commitment to protecting the interests of Big Business and focus on changing the environmental factors that foster ID theft. Big Business believes that maintaining the environmental factors as they are is in its best financial interest. Therefore, it will resist any attempts by the federal government to enact legislation regulating those factors even though that is the only way of actually reducing ID theft. Such resistance cannot be permitted to rule the day.

In his 2003 testimony before the U.S. House Subcommittee on Financial Institutions, Edmund Mierzwinski, Executive Director of the U.S. Public Interest Research Group, made this point quite clear:

> Legislation is necessary to coerce these recalcitrant firms, which generally consider a "few" mistakes and a few lawsuit settlements the cost of doing business while they ignore the real costs, both tangible and intangible, to victims. Unless banks, department stores and credit bureaus are forced by law to help prevent identity theft, they will continue in their sloppy credit-granting practices, they will continue to dismiss the problem of identity theft with their public relations campaigns and they will continue to reject the massive impact identity theft has on its consumer victims.[149]

There have been many proposals for legislation addressing ID theft, and many more will come over time. The proposals that follow

---

THREAT (October 2003), http://www.verilaw.com/presscenter/hottopics/ECIREPORTFinal.pdf

[147] *Id* at 40.

[148] *Id.*

[149] *See Concerning Affiliate Sharing Practices and the Fair Credit Reporting Act Before the Senete Banking Comm.*, 108th Cong. 14 (June 26, 2003) (statement of Edmund Mierzwinski, Consumer Program Director), *available at* http://banking.senate.gov/03_06hrg/062603/mierzwin.pdf.

do not represent an exhaustive list and might not be the most creative approaches available. They have been culled from existing proposals and represent what this author views as those most likely to have a substantial impact on the problem. They are broad proposals designed to allow the evolution of the best solutions to ID theft, to give consumers more control over their personal information and to provide disincentives to the careless storage or distribution of personal information. It should be noted that some of the proposals most likely to reduce ID identity theft are the least likely to be passed by the current federal government. Also, some broader proposals, if adopted, could render others superfluous. For example, the elimination of the SSN as the primary personal identifier for credit granting purposes would render narrower proposals limiting the use of SSNs moot.

Preemptions Preventing States From Attacking ID Theft Should Be Removed

As discussed above, the FCRA as amended by the FACTA preempts state action in many of the areas that could address the environmental contributors to ID theft. As the federal government has relinquished its role as the prime mover leading the charge against ID theft, it should at least step out of the way and let states do the job. Now is the time for the states to be the "laboratories of democracy" envisioned so long ago by Supreme Court Justice Brandeis. As this great Justice said in *New State Ice Co. v. Liebmann:*

> There must be power in the States and the Nation to remold, through experimentation, our economic practices and institutions to meet changing social and economic needs. . . . Denial of the right to experiment may be fraught with serious consequences to the Nation. It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.[150]

There is already evidence indicating that if states are left to their own devices, they will come up with effective measures to protect their citizens. The FCRA preemptions began with the 1996 amendments which specifically exempted the stronger statutes in

---

[150] New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J.,dissenting).

California, Massachusetts and Vermont.[151] These stronger laws have protected the citizens of those states and have not inhibited lenders from doing business there. In 2002, Vermont and Massachusetts had the lowest rates of consumer bankruptcy in the country, and California was below the national median.[152]The mortgage rates in these states were also below the national median.[153]

Given the creativity of the fifty legislatures, the states are bound to find new and better ways of protecting their citizens from the scourge of ID theft, while still enabling lenders and credit bureaus to operate profitability. Even now, it is clear that the states have been the leaders in attacking ID theft.[154] They have been the innovators in such areas as a consumer's right to notification of data breaches and the ability of ID theft victims to "freeze" their credit files prohibiting credit from being issued in their names.[155] Instead of lauding such accomplishments, the federal government continues to try to thwart them. With regard to data breaches, for example, the federal government is now considering a weak bill that would not contain a private right of action and would preempt stronger state laws.[156]

Barring some crisis of conscience at the federal level coupled with a well thought out national program addressing the real causes of ID theft, the states should be left to experiment. Until such a coherent national approach is developed, existing state law preemptions should be repealed and no new preemptions should be

---

[151] *See The Importance of the National Credit Reporting System to Consumers and the U.S. Economy: Hearing Before the H. Subcomm. on Financial Institutions and Consumer Credit*, 108th Cong. 3 (May 3, 2003) (statement of Professor Joel R. Reidenberg, Fordham University School of Law), *available at* http://financialservices.house.gov/media/pdf/050803jr.pdf.

[152] *Id.*

[153] *Id.*

[154] *See* CALPIRG, Financial Privacy in the States—How Consumers Benefit from Person Information Safeguards 18 (Feb., 2004), http://calpirg.org/reports/financialprivacy04.pdf.

[155] *See* Roy Mark, *Security: States Lead Congress on Breach Protections*, INTERNET NEWS, Sept. 1, 2005, http://www.internetnews.com/security/article.php/3531681; Amy C. Fleitas & Dani Arthur, *Identity Stolen? Freeze Your Credit Report*, BANKRATE.COM, July 20, 2005, http://www.bankrate.com/brm/news/cc/20030613c1.asp.

[156] *See* Roy Mark, *Business: ID Theft Bill Winds Through Senate*, INTERNET NEWS, July 28 2005, http://www.insideid.com/idtheft/article.php/3523906; Kelly Beaucar Vlahos, *ID Theft Disclosure Law Worries Advocates*, FOX NEWS, Aug. 24, 2005, http://www.foxnews.com/story/0,2933,166575,00.html.

added.

Consumers Should Be Given Control Over Their Personal Information Through an Opt-In System

Two statutory systems are available that give individuals some say in the use of their personal information. One system is an opt-in system; the other is an opt-out. Under an opt-in system, the statute presumes that individuals do not want their personal information provided to others without their knowing consent. Individuals must affirmatively give permission—opt-in—to allow their information to be transferred. The Health Insurance Portability and Accountability Act ("HIPPA")[157] establishes an opt-in system for our medical information. Under an opt-out system, personal information can be transferred unless the individual takes affirmative action to deny such transfers.

Currently, the statutory presumption is that consumers are perfectly happy with businesses being able to exchange, buy and sell their non-medial personal information. With some very significant exceptions, people are given the opportunity to opt-out of such transfers in the case of financial institutions and CRAs.[158] Privacy advocates argue that individuals do not particularly want their information to be made available without their consent, and that there should be an opt-in rather than opt-out system with few exceptions.[159] In the one case where people were given a chance to vote on this issue, they voted for opt-in.

> In 2001, citizens in North Dakota had the first and only opportunity in the nation to take a real position at the polls on the dissemination of their personal financial information. The North Dakota state legislature had just watered down financial privacy from an opt-in rule on data sharing to an opt-out rule. The citizens of North Dakota revolted. By an overwhelming 72% majority, the voters of North Dakota approved a referendum restoring the old opt-in rule and rebuking the legislature's weakening of privacy

[157] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 111936. *See also* United States Department of Health & Human Services, Summary of the HIPAA Privacy Rule 9 (May 2003), *available at* http://www.hhs.gov/ocr/privacysummary.pdf.

[158] Gramm-Leach-Bliley Act, 15 U.S.C. § 6802(b) (2000).

[159] Statement of Edmund Mierzwinski, *supra* note 149, at 3.

standards. Strong privacy clearly matters to voters and to the health of our financial and credit system.[160]

Given the daily reports of new data breaches and increased ID theft, it is likely that if the people were given an opportunity to vote on this issue today, they would strongly favor opt-in.[161]

The personal identifiers required to commit ID theft should be under the control of the individual. Consumers should have the right to agree to the transfer of that information—opt in—and in the absence of a knowing consent to its use, the information should remain private. This opt-in approach can be made to apply to financial institutions, CRAs and their affiliated companies by the amending existing law such as the Fair Credit Reporting Act[162] and Gramm-Leach-Bliley Act.[163] The protection of information in the hands of other data brokers might need a different approach.[164]

Data Brokers Should Be Regulated and Subject to Liability for Negligent Storage or Dissemination

Data brokers—businesses that collect and sell information including our personal information—are essentially unregulated. The data breach at ChoicePoint, involving the theft of 145,000 individuals' personal information, is only one example of how vulnerable our personal identifiers are in the hands data brokers.[165] If not for a 2003 California statute requiring that victims be notified that their personal information has been stolen, virtually all of the 145,000 individuals would never have been informed of their vulnerability to ID theft.[166] Blindfolding potential ID theft victims from their possible

---

[160] Reidenberg, *supra* note 151, at 4.

[161] CALPRIG, Identity Theft Prevention—What's New, http://calpirg.org/CA.asp?id2=17990&id3=CA& (last visited Feb. 4, 2006) (stating that in California, businesses pressed strong resistance to privacy laws until faced with the possibility of having the issue submitted to the voters).

[162] Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* (2005).

[163] 15 U.S.C. §§ 6801-6809.

[164] Some proposals do involve regulating data brokers under the FCRA.

[165] Center for Democracy and Technology, Recent Information Security Breaches Raise Privacy Concerns (Mar. 8, 2005), http://www.cdt.org/publications/policyposts/2005/6.

[166] Grant Gross, *ChoicePoint's Error Sparks Talk of ID Theft Law— Privacy Advocates Call for Federal Legislation After Company's Massive Data Leaks Come to Light*, PCWORLD, Feb. 23, 2005, http://www.pcworld.com/

danger cannot be permitted. Data brokers throughout the country must be required to notify victims of any breach.

Under the California law in 2005, more than sixty companies announced breaches affecting millions of U.S. residents.[167] This rash of data breaches has motivated nineteen states to pass breach notification statutes.[168] As noted above, instead of cooperating with this effort, the federal government is attempting to protect data brokers by considering a law which will not include a private right of action and will preempt strong state legislation.[169] That obstructionism must end.

Data brokers should also be held liable when they fail to adequately protect or improperly disburse our personal information.[170] The FTC has expressed concern about the behavior of data brokers,[171] but as yet nothing has been done. If data brokers can escape liability when they fail to take adequate steps to protect our personal information from getting into the hands of the wrong people, they will have little motivation to do so.[172] Even the most careful of

---

news/article/0,aid,119790,00.asp.

[167] Grant Gross, *Congress looks to Pass Data Breach Law,* INFOWORLD, Sept. 2, 2005, http://www.infoworld.com/article/05/09/02/HNcongressdata_1.html.

[168] *Id.*

[169] Robert Vamosi, *CNET Reviews, Security Watch: Congress Loves Identity Thieves*, CNET.COM, Nov. 11, 2005, http://reviews.cnet.com/4520-3513_7-6381707-1.html?tag=nl.e501.

[170] *See* Harrington v. ChoicePoint, Inc., CV 05-1294 MRP (Sept. 13, 2005) (mem.) (showing that the ChoicePoint data breach was actually a sale to criminals who had represented themselves to be legitimate businesses. In a class action brought against ChoicePoint on behalf of those individuals whose personal information was sold to these criminals, a California federal district court judge recently denied a motion to dismiss brought by ChoicePoint and held that ChoicePoint was subject to potential liability under the FCRA). *See also* Steven H. Wildstrom, *Commentary, Personal Data Theft: It's Outrageous*, BUSINESSWEEK ONLINE, Apr. 15, 2005, http://www.businessweek.com/technology/content/apr2005/tc20050415_5345_tc120.htm?chan=adsections&sub=exec_technology&campaign_id=knw_bp (on the potential liability of data brokers generally); Electronic Information Privacy Center, Letter to the Federal Trade Commission (Aug. 30, 2005), www.epic.org/privacy/iei/ftcupdate.html.

[171] *See* Consumeraffairs.com, Data Brokers Not Without Risk, FTC Testifies (May 23, 2005), http://www.consumeraffairs.com/news04/2005/ftc_data.html.

[172] The murder of Amy Lynn Boyer is one of the few cases where a data broker was found liable for providing information to the wrong individual. In that case, the information obtained was used to stalk and murder Ms. Boyer. *See* Remsburg v. Docusearch, Inc., 816 A.2d 1001 (N.H. 2003).

data repositories might become subject to data theft given the ingenuity of modern ID thieves and the computer experts who work with or for them. This proposal for liability is not addressed to careful data brokers, only careless ones. It is entirely foreseeable to data brokers that ID thieves will attempt to buy or steal our personal information. If data brokers adequately prepare for that threat, they have nothing to worry about.

The Use of Social Security Numbers Should Be Restricted

The SSN is the "key" to much of the ID theft that abounds, especially crimes involving the establishment of new accounts. This is because the SSN is recognized as the primary personal identifier for extending credit.[173] The development of a new, less vulnerable credit personal identifier will take time and a great deal of thought. In the meantime, restrictions on the use of SSNs are necessary to reduce ID theft.

Congress has been called upon to lessen social security number use:

> If the SSN is available in fewer places, on fewer documents and used for fewer commercial transactions or database identifiers when it shouldn't be, identity thieves as well as stalkers and even terrorists will be less able to harvest it for misuse.[174]

Proposals on restricting the sale and use of SSNs come up from time to time.[175] Several general principles can be derived from these proposals. First, the trafficking in SSNs must be eliminated. It should be against the law to transfer, buy or sell SSNs. This principle should apply to both the public and private sector. It would apply, for example, to data brokers and the CRA "credit header" exception.[176]

---

[173] For a discussion of SSNs, see Robert Ellis Smith, *Social Security Numbers: Uses and Abuses*, PRIVACY J. (2002), *available at* http://www.simson.net/ref/databasenation/SSNReport2001.pdf.

[174] *See* Mierzwinski, *supra* note 149.

[175] *See Protecting the Privacy of Consumers' Social Security Numbers: before the H. Energy and Commerce Subcomm. on Commerce, Trade, and Consumer Protection* (Sept. 28, 2004) (testimony and statement for the record of Chris J. Hoofnagle, Associate Director, Electronic Privacy Information Center), http://www.epic.org/privacy/ssn/ssntestimony9.28.04.html.

[176] Letter from U.S. Public Interest Research Group, Endorsing Nelson-Markey Proposals (S 500/HR 1080) Regulating Information Brokers (Mar. 8,

Those that continue to traffic in SSNs should be subject to both criminal and civil liability. On the civil side there must be a private right of action,[177] including potential injunctive relief to prevent similar conduct in the future.[178]

A second way to prevent the overuse and abuse of SSNs is to forbid businesses or government agencies from requiring individuals to provide their social security numbers. Except for such items as taxes, Social Security, Medicare, and Medicaid,[179] no person should be compelled or coerced into providing a SSN for any transaction.[180] This restriction would include applications for credit, applications for employment and requests to receive a copy of one's credit report.[181]

Schools and colleges are another potential source of SSNs. Many schools use SSNs as student identifiers, and the Department of Education reports that nationally fifty percent of student grades are posted by SSNs.[182] Laws restricting the use of SSNs should address this issue, especially considering the number of colleges and universities that have been subject to data breaches.[183] If these restrictions on the trafficking in SSNs, the ability of businesses or government agencies to demand SSNs and the use of SSNs by educational institutions were enacted into law, they would have a substantial impact of ID theft.

2005), http://www.pirg.org/consumer/pdfs/pirgendorsesnelsonmarkey.pdf.

[177] Such a private right of action could be similar to the Truth in Lending Act, 15 USC. § 1601 *et seq.*, which provides for a minimum amount of damages,15 USC § 1640(a)(2)(A), and reasonable attorney's fees, 15 USC § 1640(a)(3).

[178] Injunctive relief is essential where there is a common practice that is likely to reoccur.

[179] These areas and others, including the Department of Defense, still have significant SSN problems. Because of the diverse nature of these areas, addressing these problems will require different approaches. *See* ScienceDaily.com, Medicare, Defense Cards a Boon to ID Theft, (Sept. 19, 2005), http://www.sciencedaily.com/upi/?feed=TopNews&article=UPI-1-20050917-20070200-bc-us-identitytheft.xml.

[180] *See* Mierzwinski, supra note 149.

[181] *Id.*

[182] *See* Alex Sellinger, *Students are Often the Victims of Identity Theft; Fraud*, THE CAVALIER DAILY, Oct. 31, 2005, www.cavalierdaily.com/CVArticle.asp?ID=24955&pid=1357.

[183] *See, e.g.*, Daniel, *supra* note 25; OhioNewsNow, *supra* note 25.

Consumers Should Have Private Rights Of Action Including Class Actions and Injunctive Relief

There are two primary methods of enforcing consumer protection statutes. One method is by governmental agency action. Although agency action can be very powerful, it is subject to funding constraints and, to some extent, the philosophy of the administration in power.[184] Even if given resources and full reign, agencies must often reserve their intervention for the most egregious cases or those which will have the largest impact.

The other way of enforcing consumer statutes is by authorizing consumers subjected to a violation of a statute to sue for its breach—by creating a private right of action in the statute. People who prosecute such suits are called "private attorneys general" because they act, in part, as an enforcement agent on behalf of the government.[185] This can be a very effective, low-cost means of assuring that the goals of a statute are met. At the same time, it enables at least the one victim suing to receive compensation. Some private right of action statutes also provide for class actions and injunctive relief. Class actions enable the injured consumer to sue on behalf of all consumers who have been injured by the same conduct, and injunctive relief would prohibit the defendant from engaging in similar conduct in the future. While consumer groups clamor for private rights of action in statutes designed for their protection, businesses, not surprisingly, take the opposite position.

Two of the most important statutes affecting ID theft are the FCRA[186] and the GLBA.[187] The GLBA has no private right of action.[188] The FCRA has no private right of action in certain areas,[189]

---

[184] Consider how much governmental energy went to the Federal Communications Commission after Janet Jackson had her "wardrobe malfunction" at the Super Bowl in 2004.

[185] *See, e.g.*, William B. Rubenstein, *On What a Private Attorney General is - And Why it Matters*, 57 VAND. L. REV. 2129(2004), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=743544; Pamela S. Karlan, *Disarming the Private Attorney General*, 2003 U. ILL. L. REV. 183, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=308220; Gary M. Victor, *The Michigan Consumer as a Private Attorney General*, 4 COLLEAGUE 13 (1991).

[186] 15 U.S.C. §§ 1681 *et seq.*

[187] *Id.*

[188] *Id.*

[189] *See* National Consumer Law Center ("NCLC"), Analysis of the Fair and Accurate Credit Transactions Act of 2003, http://www.nclc.org/initiatives/

and a right of action in other areas that is so weak that it can hardly be called a right of action.[190] Even where the FCRA provides for a right of action, it does not provide for class actions or injunctive relief.[191]

For example, consumers are now entitled to notice when a financial institution is furnishing negative information about them.[192] Assuming a case where no notice is given, the information furnished was the result of ID theft and the ID theft victim suffers damages; the ID theft victim has no right to sue the financial institution. If this financial institution has a pattern and practice of refusing to send out notices, even if there were a private right of action, the injured consumer cannot sue on behalf of others injured by the practice and cannot sue for injunctive relief ordering the financial institution to comply with the FCRA in the future. These remedies would only be available in an action brought by a governmental agency.[193]

By strengthening private rights of action and by enacting private rights of action where none currently exist, ID theft can be reduced and victims compensated. These rights of action should include the right to recover actual damages or a minimum statutory amount if actual damages are less, together with reasonable attorneys' fees.[194] They must also include the right to pursue class and injunctive relief. If a business is engaging in conduct that it considers profitable even though it knows or should know that the conduct is in violation of a statute, the downside of having to "pay off" the few individuals that sue for the violation is not likely to deter future violations. If, on the other hand, they realize that they can be forced to pay all injured consumers back and/or they can be enjoined

---

facta/contents/nclc_analysis_content.html#1#1 (last visited Mar. 6, 2006).

[190] The FCRA limits liability for certain violations of the FCRA with a qualified immunity provision that allows consumers to bring certain state law claims only if the consumer shows that the information was furnished with "malice or willful intent to injure" *Id.* This high standard substantially dilutes the right of action in those areas.

[191] There is a right of action to sue for both negligent and willful conduct. *See* 15 U.S.C. § 1681(o); 15 U.S.C. § 1681(n).

[192] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 *et seq.*

[193] In fact, the FACTA created a limitation of a state's ability to sue for damages on a class basis. In certain areas, a state must first sue for injunctive relief, and can only sue for damages for a later violation of the injunctive order. *See* NCLC, *supra* note 123.

[194] Providing for reasonable attorneys' fees is necessary in order to induce qualified attorneys to take such cases. This is called "fee shifting."

from engaging in such conduct in the future, it is more likely that they will restrain their conduct in the first place. Businesses are in business to make profits. Only when the potential monetary losses from ID theft promoting behavior exceed the potential profits from that conduct, can we expect the conduct to cease.

Conclusion

We are in the midst of an ID theft crisis.[195] Ten million people were victims of ID theft in 2003 and another ten million in 2004, resulting in losses of over $50 billion in each of those years.[196] The old methods of stealing identities[197] are giving way to more sophisticated methods of data theft over the Internet.[198] Data breaches involving the theft of over 50 million identities have taken place in less than a year.[199] Unless the environmental factors that contribute to ID theft are addressed, ID theft will continue to plague our society, causing substantial economic and emotional damage.

The factors that contribute to the rise in ID theft are not difficult to identify. Since personal information is the "lifeblood" of ID theft, activities that make that information available to ID thieves are essentially to blame. One primary ID theft facilitator is our information age, which has put enormous amounts of personal information in the hands of data brokers, financial institutions, CRAs, retailers and other institutions—information that can be bought, sold or stolen. Other factors include the ability of lenders to pass the cost of ID theft on to the public, the behavior of lenders and CRAs, the use of SSNs as the universal personal identifier, and, perhaps most importantly, the refusal of the federal government to address the problem in any meaningful way.

To date, there has been little federal action addressing the environmental forces that contribute to ID theft. Thus far, business interests have been able to thwart attempts to cure these environmental causes. To facilitate a reduction in ID theft, the federal government must enact new legislation and remove existing laws that prohibit the states from experimenting with their own, unique

---

[195] *See, e.g.*, Javelin, *supra* note 6, at 7.

[196] *Id.*

[197] *Id.*

[198] *Id.*

[199] *See* Privacy Right Clearinghouse, *supra* note 21.

solutions to the ID theft crisis. Proposals for changing the ID theft environment include abolishing the preemptions in the FCRA which prevent states from enacting stronger ID theft protections, switching to an opt-in system enabling consumers to take charge of their personal information, regulating data brokers so that they will be liable for the improper storage or distribution of personal information, restricting the trafficking in SSNs and providing private rights of action that will allow ID theft victims to sue for damages, class relief and injunctive relief when their rights are violated.

***