

## HOW THE INTERNET HAS EXPANDED THE THREAT OF FINANCIAL IDENTITY THEFT, AND WHAT CONGRESS CAN DO TO FIX THE PROBLEM

By Ian Heller\*

### INTRODUCTION

Every few months a news story appears revealing the theft or loss of computer hard drives containing sensitive financial information of millions of bank and consumer credit report customers.<sup>1</sup> Identity theft is the fastest growing crime in the United States,<sup>2</sup> known by many as “the signature crime of the digital era.”<sup>3</sup> The Federal Trade Commission (the “FTC”) estimates that thieves appropriate the names, addresses, social security numbers, and credit card numbers of about 10 million Americans each year.<sup>4</sup> The annual price tag is an alarming \$48 billion to businesses and \$5 billion to consumers.<sup>5</sup> Every three seconds, someone falls victim to the various scams used by thieves to steal identities.<sup>6</sup> Stolen information is “used by thieves to open new accounts, secure loans, and otherwise lead parallel and often luxurious lives.”<sup>7</sup> As David

---

\* J.D. and M.B.A. Candidate, Stetson University College of Law, December 2007. Upon graduation and successful admittance to the Florida Bar, the author hopes to begin a career in Public Service

1. Bruce Kauffman, *NCTimes.Com, Hard drive with personal data missing from CSUSM*, [http://www.nctimes.com/articles/2004/08/04/news/top\\_stories/23\\_18\\_308\\_3\\_04.txt](http://www.nctimes.com/articles/2004/08/04/news/top_stories/23_18_308_3_04.txt) (Aug. 3, 2004); Tom Krazit, *InfoWorld, Notebook theft could expose personal data*, [http://www.infoworld.com/article/04/12/22/HNtheft\\_1.html](http://www.infoworld.com/article/04/12/22/HNtheft_1.html) (Dec. 22, 2004).

2. *Examining the Financial Service Industry's Responsibilities and Role in Preventing Identity Theft and Protecting Sensitive Financial Information: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 109<sup>th</sup> Cong. 2-3 (2005) [hereinafter *Hearing*] (statement of Senator Jack Reed), available at, [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109\\_senate\\_hearing&docid=f:31069.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_senate_hearing&docid=f:31069.pdf).

3. Michael McCutcheon, *Identity Theft, Computer Fraud and 18 U.S.C. § 1030(G): A Guide to Obtaining Jurisdiction in the United States for a Civil Suit Against a Foreign National Defendant*, 13 Loy. Consumer L. Rev. 48, 48 (2001).

4. Tom Zeller Jr., *For Victims, Repairing ID Theft Can Be Grueling*, N.Y. TIMES, Oct. 1, 2005, at C1, available at <http://www.nytimes.com/2005/10/01/technology/01theft.html?pagewanted=1&ei=5070&en=8d96a81f04022898&ex=1187236800>.

5. *Hearing*, *supra* note 2, at 4.

6. Mich. S. J., 93<sup>rd</sup> Leg., Reg. Sess. 200 (2005).

7. Zeller, *supra*, n. 4.

Young, co-chair of the privacy law group at Lang Michener LLP noted, “Individuals in today’s world are very, very exposed to privacy theft. . . There are instances occurring on quite a regular basis, and they never reach the media.”<sup>8</sup>

The current methods used to combat financial identity theft are incapable of achieving any real success because they focus on punishment. Currently, financial institutions are only liable to their customer-victims in limited circumstances and offenders regularly escape justice. As a result, monetary penalties and threats of imprisonment have done little to curb the monumental increase in identity thefts over the last decade. This note argues in favor of shifting the policy of dealing with identity theft from punishment to deterrence, and shifting the burden of its prevention from financial institutions to points-of-sale at retail, online, and commercial establishments.

Part I of this article begins with an exploration of identity theft, focusing in particular on the financial and emotional burden felt by victims, and how the proliferation of Internet use has expanded its threat. In Part II, the article identifies domestic and international efforts currently employed to deal with financial identity theft, and where these efforts fall short. Finally, Part III proposes two alternative solutions to combat financial identity theft: one utilizing the power of free markets and the other relying upon secure biometric technology, both focused on deterrence rather than punishment.

## PART I: THE PROBLEM

### *Financial Identity Theft, an Overview*

Financial identity theft (“ID theft”) is “a crime in which an imposter obtains key pieces of personal identifying information. . .and uses them for their own personal gain.”<sup>9</sup> Information can be stolen as a result of inadequate security measures on the part of large holders of personal data, from rouge office employees, through a creative con man, by the casual use of a photocopy machine,<sup>10</sup> or even from a lost wallet ending up in the wrong hands.<sup>11</sup> An ID thief needs very little to steal an identity: the information needed can be as simple as a first and last name, a home address, and either a social security number or a credit card number.<sup>12</sup>

There are two major categories of ID theft: the misuse of personal

---

8. Sinclair Stewart, *Privacy Breaches*, (Jan. 24, 2007) <http://www.theglobeandmail.com> (available in LEXIS, News Library).

9. The Identity Theft Resource Center, *Home*, <http://www.idtheftcenter.org> (last visited Apr. 16, 2007).

10. CNN.Com, *Experts warn of identity theft risk*, <http://www.cnn.com/2007/TECH/ptech/03/14/photocopier.risks.ap/index.html> (Mar. 15, 2007).

11. *Murray v. Bank of Am. N. Am.*, 580 S.E.2d 194, 196 (S.C. Ct. App. 2003).

12. Brett Nauman, *Identity crisis: Sandi Cullers is a victim of identity theft. Will you be next?* The Pantagraph (Bloomington, Illinois) (Oct. 1, 2005) (available in LEXIS, News Library).

accounts and the creation of new accounts in the victim's name.<sup>13</sup> Almost 60% of victims 'don't learn of the fraud until a full month after the crime has occurred,<sup>14</sup> usually when the victim attempts to obtain credit, for example, by securing an equity loan or mortgage. ID theft investigations typically commence when the victim's credit report reveals a delinquent payment history or outstanding debts that are not attributable to her actions.

ID theft hurts more than just the obvious victim. The financial institution that issued the fraudulent account is typically forced to absorb the financial loss.<sup>15</sup> As a result, the "legal victim" is the institution itself, which severely restricts the rights of the innocent individual, or "true-name victim," whose identity was stolen.<sup>16</sup> Furthermore, the impact of ID theft goes well beyond finances; until theft can be proven, the victim is responsible for all actions carried out in her name. Higher interest rates, one result of negative credit report entries, often penalize victims<sup>17</sup> who must invest thousands of hours each year in charge disputes and navigating red tape to clean up their credit.<sup>18</sup> The hardest thing, one victim said, was "feeling powerless to do anything once the fraud started to happen."<sup>19</sup> If a victim sues, it is likely that damages sought will stem from, among other things, the onslaught of emotional distress.

Despite the creation of 25 new state laws and the introduction of 34 Congressional bills in 2006 intended to protect personal information,<sup>20</sup> only one in seven hundred ID thieves are successfully apprehended and even fewer are seized "red handed."<sup>21</sup> According to Tom Zeller of *The New York Times*, prosecutions are rare; police investigations often start years after the fraud has occurred and are repeatedly frustrated by costly and time-intensive inquiries.<sup>22</sup> Investigators must sift through hundreds of credit transactions in order to ascertain which are legitimate and which are not. Even then, evidence is typically insufficient to provide law enforcement with any real clues as to the

---

13. *Examining the Financial Services Industry's Responsibilities and Role in Preventing Identity Theft and Protecting Sensitive Financial Information*, *supra* n. 2.

14. The Fed. Trade Comm'n, *Identity Theft Data Clearinghouse, Identity Theft Victim Complaint Data: Figures and Trends, January 1-December 31, 2005*, 8, [http://www.consumer.gov/idtheft/pdf/clearinghouse\\_2005.pdf](http://www.consumer.gov/idtheft/pdf/clearinghouse_2005.pdf). (Last Visited Jan. 25, 2006).

15. *Identity Theft: The Causes, Costs, Problems and Consequences and Potential Solutions: Hearing Before the H. Subcomm. On Tech., Info., Policy, Intergovernmental Relations and The Census*, 108<sup>th</sup> Cong. (2004), available at <http://a257.g.akamaitech.net/7/257/2422/25feb20051230/www.access.gpo.gov/congress/house/pdf/108hr98486.pdf>

16. *Id.*

17. *Legge v. Nextel Comm.*, No. CV 02-8676 DSF (VBKx), 2004 U.S. Dist. LEXIS 30333, \*9 (D. Cal. June 25, 2004).

18. *Murray*, 580 S.E.2d at 196-197.

19. *Hearing*, *supra*, note 2 at 4.

20. The Identity Theft Resource Center, *Identity Theft Resource Center's 2006 Year in Review and Predictions for 2007*; "Contrary to popular opinion, 2006 was not the Year of the Breach," states Jay Foley of the Identity Theft Resource Center, "rather it was the year when breaches received a great deal of public awareness," <http://www.pnnewswire.com> (Jan. 4, 2007) (available in LEXIS, News Library).

21. Zeller, *supra*, n. 4.

22. *Id.*

thief's identity.

### *The Internet*

The proliferation of the Internet has only increased the ease of ID theft because of the relative anonymity of operating online. No other marketplace in the world has as many vendors and service providers so readily available, with more entering the market every day. E-commerce has its own "Black Monday" shopping frenzy.<sup>23</sup> In the simplest of transactions, a consumer selects the goods she desires and enters her name, billing (and/or shipping) address, and major credit card information. But therein lies the problem. Your favorite retailer's website cannot tell the difference between a legitimate customer and an identity thief if both correctly enter the customer's first and last name, billing address, and major credit card information. Internet usage increases the convenience and productivity of daily life, but in gaining these benefits, internet users "open [themselves] up to the exploitation of that information by criminals and by others."<sup>24</sup>

At the turn of the century, 500,000 Americans had become victims of ID theft.<sup>25</sup> According to Senator Jack Reed of Rhode Island, the number of ID thefts ballooned to 10 million Americans just four years later.<sup>26</sup> By the year 2005, identity theft represented the largest category of fraud complaint on file with the FTC's fraud database, the Consumer Sentinel, constituting 37% of all fraud complaints.<sup>27</sup> As the world embraces online transactions with increasing zeal, security is struggling to keep pace. Unfortunately, at least one study has found that the emotional impact of ID theft is clinically comparable to the impact on victims of violent crimes.<sup>28</sup> As one victim lamented, "it was so much easier in the old days when they just knocked you over the head in a dark alley and stole your wallet."<sup>29</sup>

Of all the potential ways to use the Internet to defraud consumers, one stands out as the most notorious, complex, and widely-used method of ID theft: "phishing". In 2003, the FBI labeled phishing as "the hottest, and most troubling, new scam on the Internet."<sup>30</sup> Phishing, or "spoofing," frauds attempt to make Internet users believe they are receiving e-mail from a specific, trusted

---

23. VeriSign, *Internet Commerce Grows 88 Percent by Dollar Volume and 39 Percent by Transaction Volume: Fraud Remains a Concern*, (Feb. 25, 2005). [http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2005/page\\_028572.html](http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2005/page_028572.html).

24. *Hearings, supra*, note 2 at 3.

25. 147 Cong. Rec. S6129 (daily ed. June 12, 2001) (statement of Sen. Jim Bunning).

26. *Hearings, supra*, note 2 at 3; Zeller, *supra*, n. 4.

27. The Fed. Trade Comm'n, *supra* note 16 at 3.

28. Foley, *supra*, n. 9 at 35.

29. Paul A. Greenberg, *E-Commerce Times, Identity Fraud - The Great E-Commerce Roadblock*, <http://www.ecommercetimes.com/story/11932.html> (July 12, 2001).

30. *Internet Fraud Hits Seniors: As Seniors Venture into the Web, the Financial Predators Lurk and Take Aim: Hearing Before the S. Spec. Comm. On Aging*, 108<sup>th</sup> Cong. 2 (2004) (statement of David Jevans, Chairman, Anti-Phishing Working Group), available at <http://aging.senate.gov/events/hr120dj.pdf>.

source in an effort to obtain personal or financial information over the Internet.<sup>31</sup> The attack can come in different forms. Often the scammer will use “URL spoofing” to mimic a trusted website.<sup>32</sup> The scammer then directs consumers to seemingly genuine websites, giving the transaction an air of legitimacy, and lessening the likelihood that a consumer would realize that a fraud has been perpetrated.<sup>33</sup> In 2006, “about 109 million U.S. adults received phishing e-mails, up from 57 million in 2004;” about one in six phishing e-mails are opened – a better rate than for e-mails from legitimate businesses.”<sup>34</sup>

While phishing has been a problem since the debut of the Internet, as Katherine Brinton’s experience indicates, the level of sophistication associated with modern attacks is overwhelming. *USA Voice*, an online news site self-proclaimed as “Honest and Unfiltered,” features news articles and commentary on national issues and considers itself “the world’s fastest growing news organization.”<sup>35</sup> So it is understandable why Ms. Brinton, an aspiring journalist, did not think twice about the email she received indicating that *USA Voice* was looking for reporters with “excellent writing skills” and an “innate ability to find the truth.”<sup>36</sup> After all, Brinton posted her resume on Monster.Com and CareerBuilder.com nine months earlier, websites dedicated to pairing job seekers with employers.<sup>37</sup> Following the web link provided to her in the e-mail, Brinton was prompted to fill out an online “application,” which required her name, address, and telephone number.<sup>38</sup> Although the job offers never came, she later began receiving a stream of unsolicited e-mails hawking erectile dysfunction medicine and penny stocks.<sup>39</sup> Brinton was the victim of a sophisticated phishing technique. According to Jeff Wilbur, Vice-President of marketing for the e-mail security firm Iconix, these types of attacks “might be the final piece of the puzzle” that phishers need to exploit an individual’s identity.<sup>40</sup> As Ms. Brinton’s experience proves, phishers go to great lengths to earn and exploit consumer trust, and even e-mails that appear solicited can easily contain a phishing danger.

Another new development in phishing is “malcode”, through which the Internet scammer sends the consumer to a fake URL that hosts a malicious

---

31. *Associated Bank-Corp. v. Earthlink, Inc.*, No. 05-C-0233-S, 2005 U.S. Dist. LEXIS 20184, \*2-3 (D. Wis. Sept. 13, 2005).

32. United States Dept. of Justice, *Special Report on “Phishing”* 1 (2004), <http://www.usdoj.gov/criminal/fraud/docs/Phishing.pdf>.

33. The Anti-Phishing Working Group, *Proposed Solutions to Address the Threat of Email Spoofing Scams* 3 (Dec. 12, 2003), [http://www.antiphishing.org/Proposed%20 Solutions%20to%20Address%20the%20Threat%20of%20Email%20Spoofing%20Scams%20White%20Pa per.pdf](http://www.antiphishing.org/Proposed%20Solutions%20to%20Address%20the%20Threat%20of%20Email%20Spoofing%20Scams%20White%20Paper.pdf).

34. Annys Shin, *It’s Another Phish Story: Job Seekers Take the Bait*, *The Washington Post*, Feb. 11, 2007, available at LexisNexis, News Library.

35. *Id.*

36. *Id.*

37. *Id.*

38. *Id.*

39. *Id.*

40. *Id.*

software application or contains secretly downloaded malicious scripts,<sup>41</sup> also known as “trojan horses.”<sup>42</sup> This happens when the attackers succeed in infiltrating the domain name server (“DNS”) which stores the actual numerical equivalent of a Web site address. When a web-surfer enters a web address into a browser, for example “www.buyclothesnow.com”, the DNS interprets the common name<sup>43</sup> and changes it to the Internet Protocol address (the “IP address”), a unique set of numbers and periods that functions as a website’s mailing address.<sup>44</sup> Consequently, the IP address for “www.buyclothesnow.com” might actually look like “216.27.61.137,” the words being solely for human comfort.<sup>45</sup> Consider what happens if an identity thief manages to convince an individual to download a program that secretly reroutes “www. buyclothesnow.com” to the thief’s phony site located at “222.56.99.554.” Although the individual might think they are buying clothes on a secure website, in actuality, the buyer is handing her credit and home shipping address over to the thief on a silver platter.

Another form of malcode involves the installation of “key-loggers,”<sup>46</sup> which send information from the consumer’s computer to the attacker when specific, predetermined sites are accessed.<sup>47</sup> Key-loggers remain inactive until the consumer accesses and provides, for example, Amazon.com or Ebay.com with credit card information. Modern phishing scams such as this, no longer need active participants; now phishers can lay dormant for weeks, months, or years, waiting until the victim clicks their way right into a trap.

As so succinctly put by the Home PC Firewall Guide, “The only way to make a home computer 100% secure is to turn it off or disconnect it from the Internet. The real issue is how to make one 99.9% secure when it is connected.”<sup>48</sup> Firewall technology, which has been adopted by Microsoft Windows,<sup>49</sup> attempts to shield a “computer or network from malicious or unnecessary Internet traffic”<sup>50</sup> by distinguishing between desired Internet

---

41. David McGuire, *Senate Bill Targets “Phishers”*, The Washington Post, July 12, 2004, available at 2004 WLNR 5882957.

42. SearchSecurity.Com Definitions, *Trojan Horse*, [http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci213221,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html) (last visited July 10, 2006).

43. *How Web Servers Work*, HowStuffWorks, January 12, 2001, <http://computer.howstuffworks.com/web-server6.htm>.

44. *What is an IP address?*, HowStuffWorks, January 12, 2001, <http://computer.howstuffworks.com/question549.htm>.

45. *Id.*; see also *How Web Servers Work*, *supra*, at n. 44.

46. SpywareGuide, *Intro to Greynets and Spyware*, [http://www.spywareguide.com/txt\\_intro.php](http://www.spywareguide.com/txt_intro.php) (2006).

47. SpywareGuide, *Definition of Keylogger*, [http://www.spywareguide.com/category\\_show.php?id=3](http://www.spywareguide.com/category_show.php?id=3) (2006).

48. Stephen Henry Markus, *Home PC Firewall Guide*, <http://www.firewallguide.com> (last visited July 14, 2007).

49. Microsoft Windows XP, *Using Windows Firewall*, <http://www.microsoft.com/windowsxp/using/networking/security/winfirewall.mspx> (last visited Aug. 15, 2006).

50. United States Computer Emergency Readiness Team, *Understanding Firewalls*, <http://www.us-cert.gov/cas/tips/ST04-004.html> (last visited February 28, 2007).

connections and dangerous ones.<sup>51</sup> It should be noted, however, that the preferred method of phishing attack, spurious emails, are uniquely resistant to firewall technology because “a firewall offers little to no protection against viruses that work by having you run the infected program on your computer, as many email-borne viruses do.”<sup>52</sup> In other words, firewalls and Internet-security programs are not sophisticated enough to prevent you from being deceived.

## PART II: CURRENT ATTEMPTS IN DEALING WITH IDENTITY THEFT

### *Federal Laws*

The challenges presented by ID theft have not been neglected by Congress.<sup>53</sup> The Fair Credit Reporting Act (the “FCRA”)<sup>54</sup> and the Identity Theft Penalty Enhancement Act (the “ITPEA”) were passed specifically to combat ID theft.<sup>55</sup> Through these statutes, Congress created two classes of ID theft crimes: aggravated crimes and non-aggravated crimes. Additionally, because of the unique role that financial institutions play in the regulation of credit and personal information, liability is no longer reserved exclusively for the perpetrator of ID theft.

#### **The Fair Credit Reporting Act**

The financial services industry represents 89.3% of all information seizures in phishing frauds.<sup>56</sup> FCRA, overseen by the FTC,<sup>57</sup> is intended to ensure public confidence<sup>58</sup> in a banking system utilizing credit-based transactions. In so doing, the FCRA requires “consumer reporting agencies [to] adopt reasonable procedures for meeting the needs of commerce for consumer credit and other information in a manner which is fair and equitable to the consumer, with regard to . . . confidentiality.”<sup>59</sup>

#### **Process**

A consumer may sue for a violation of the FCRA’s detailed reporting requirements. The FCRA places distinct obligations on three types of entities: 1) consumer reporting agencies (“CRAs”); 2) users of consumer reports; and 3) furnishers of information to consumer reporting agencies. CRAs “play a vital

---

51. Microsoft Windows XP, *supra* note 55.

52. United States Computer Emergency Readiness Team, *supra* note 51.

53. H.R. Rep. No. 109-454, pt. 1, (2006); see Hearings, *supra* note 2.

54. 15 U.S.C.A. §§ 1601, 1603, 1681 (2004).

55. H.R. Rep. No. 109-742, at 66-67, 146 (2007).

56. The Anti-Phishing Working Group, *Phishing Attack Trends Report 4* (Dec. 2005), [http://www.antiphishing.org/reports/apwg\\_report\\_DEC2005\\_FINAL.pdf](http://www.antiphishing.org/reports/apwg_report_DEC2005_FINAL.pdf).

57. Katy K. Liu, *Fair and Accurate Credit Transactions Act Regulations: Disclosures, Opt-Out Rights, Medical Information Usage, and Consumer Information Disposal*, available at 2 ISJLP 715, 715 (2006).

58. 15 U.S.C.A. § 1681(a)(1), (3).

59. 15 U.S.C.A. § 1681(b).

role in assembling and evaluating consumer credit” for the purpose of furnishing consumer reports to third parties.<sup>60</sup> All users of credit information who use the information contained in a consumer report to deny credit or increase credit rates are required to “supply the consumer with the name and address of the [CRA] that furnished the report.”<sup>61</sup> Although a furnisher of information is not defined within the act, “common sense dictates that the term would encompass an entity . . . which transmits information concerning a particular debt owed by a particular consumer” to a CRA.<sup>62</sup>

CRA's are required to investigate the accuracy of any information disputed by a consumer.<sup>63</sup> If inaccurate information is uncovered, the CRA must correct the mistake and inform the furnisher of the modification.<sup>64</sup> For example, suppose an individual dreams to open up her own coffee franchise. She saves money for years, does her research, scouts a location, and identifies top management. To make this business a reality, the entrepreneur needs an influx of \$50,000. Unfortunately, when she applies for a loan, the bank tells her that she is an unreliable investment because she has been delinquent on payments and her new checking account is overdrawn. In disbelief, she begins to investigate. As it turns out, when she lost her wallet five months ago, her identity was appropriated and used to fund an elaborate shopping spree that stretched across three states. If the individual reports this information to her bank, it triggers a duty on the part of financial institutions. Pursuant to the FCRA, the bank must inform its CRA of the dispute, who in turn has its own investigatory duties (discussed *infra*). Through an often time-consuming process, the CRA is able to separate the individual's transactions from the thief's. The CRA then discloses this information to the bank and modifies the banker's credit report to prevent further injury. Through these efforts, the FCRA attempts to put the individual back on an even playing field. A failure on the part of the FCRA to put the individual back on an even playing field could become the basis for “civil liability for willful or negligent violations of the FCRA”<sup>65</sup> (discussed *infra*).

In 2003, the Fair and Accurate Credit Transactions Act (the “FACTA”) amended the FCRA. Under FACTA, once a consumer has a good faith belief that she is or is about to become a victim of ID theft, she may demand that her CRA place a fraud alert on her file, which is accessible by all users of credit.<sup>66</sup> Additionally, the CRA must provide the consumer with at least two copies of

---

60. 15 U.S.C.A. § 1681a(2).

61. 15 U.S.C.S. § 1681m(d)(2); *Lema v. Citibank N. Am.*, 935 F.Supp.2d 695, 698 (D.Md. 1996).

62. *Carney v. Experian Info. Solutions, Inc.*, 57 F.Supp.3d 496, 501 (W.D. Tenn. 1999).

63. *Pinson v. Equifax Credit Info. Servs., LLC*, 2007 U.S. Dist. LEXIS 5171, at \*6 (N.D. Okla. Jan. 24, 2007).

64. *Jarrett v. Bank of Am.*, 421 F. Supp. 2d 1350, 1353 (D. Kan. 2006).

65. *Carney*, 57 F. Supp. 2d at 500.

66. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 112, 117 Stat. 1952, 1955-56 (2003).

her credit report reflecting the fraud alert,<sup>67</sup> and is prohibited from reporting negative information that results from the alleged ID theft.<sup>68</sup> *Murray v. Bank of America* provides an excellent illustration of how such an alert can protect consumers.<sup>69</sup> In 1997, after Margaret Murray lost her wallet, an imposter opened a checking account in her name, writing more than \$7,000 in fraudulent checks.<sup>70</sup> When Murray discovered the fraud, she ordered the bank to close the account and inform the merchants who had been paid with the fraudulent checks of the mistake.<sup>71</sup> Neither occurred.<sup>72</sup> Had FACTA been established, Murray's experience might have been different. A fraud alert could have halted further fraudulent use of Murray's identity and could have helped locate Murray's imposter. Once flagged, use of a bad check acts as a homing beacon for law enforcement.

Despite this progression, true ID theft protection is not a reality for most victims. As amended, the FCRA ignores a critical problem; victims, on average, don't learn of ID theft until months after its occurrence.<sup>73</sup> According to the Consumer Sentinel database, in 2005, almost 60% of ID theft victims had not contacted the CRA to place a fraud alert on file.<sup>74</sup> Consumers are effectively defenseless until they make the first move. Only then may they realize the benefits of a fraud alert and credit report. Victims of online fraud are especially sensitive to this problem. Phishers lure victims into disclosing their personal data through elaborate masquerades. The deception, by its nature, convinces the victim that she is dealing with a legitimate business. So how is a phishing victim to recognize that she needs the benefit of the protections granted by the amended FCRA? A phishing victim is "unlikely to seek out a credit report until she notices suspect charges on her account."<sup>75</sup> An FTC ID theft survey revealed that when the fraud is not discovered promptly, the damage to the victim becomes increasingly difficult to repair.<sup>76</sup> FACTA, while commendable in spirit, provides only meager protections against ID theft.

Under the FCRA, furnishers receive slightly different treatment than CRAs.<sup>77</sup> Furnishers act as gatekeepers. They are responsible for providing

---

67. *Id.* at 1957.

68. *Id.* at 1964.

69. *Murray v. Bank of America*, 354 S.C. 337 (S.C. Ct. App. 2003).

70. *Id.* at 341.

71. *Id.* at 342.

72. *Id.*

73. Mary L. Boland, *Crime Victim's Guide to Justice: Legal Survival Guides* 84, SPHINX PUBLISHING (Naperville, Ill.) (Sept. 2001); see Zeller, *supra* note 4.

74. The Federal Trade Commission, *Identity Theft Victim Complaint Data Figures and Trends January 1-December 31, 2005* fig. 9, [http://www.consumer.gov/idtheft/pdf/clearinghouse\\_2005.pdf](http://www.consumer.gov/idtheft/pdf/clearinghouse_2005.pdf) (Jan. 25, 2006).

75. Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259, 280 (2005).

76. Federal Trade Commission, *supra* note 74.

77. *Stafford v. Cross Country Bank*, 262 F. Supp. 2d 776, 782 (W.D. Ky. 2003).

accurate information to CRAs<sup>78</sup> and for investigating consumer disputes.<sup>79</sup> Upon receipt of a dispute notice from a CRA, the furnisher must: 1) investigate the disputed information; 2) review all relevant information provided to it by the CRA; 3) report the results of its investigation to the CRA; and 4) report the results to all other agencies to which the information was originally furnished if an inaccuracy is discovered.<sup>80</sup>

Although such investigation could provide a victim with relief and support, it is only compulsory when the dispute notice originates with the CRA.<sup>81</sup> Furthermore, although both entities are equally liable for actual damages and attorney's fees, some federal courts have interpreted the FCRA to prohibit a private right of action against furnishers.<sup>82</sup> At least one court held that the distinction, even though seemingly cold and impractical, is valid under a plain reading of the statute.<sup>83</sup> This means that, although the statute "broadly imposes duties" against furnishers, notice from the consumer herself does not trigger furnisher liability.<sup>84</sup> The Ninth Circuit explained the difference in treatment as one that "can be inferred from the structure of the statute that Congress did not want furnishers of credit information exposed to suit by any and every consumer dissatisfied with the credit information furnished."<sup>85</sup>

### Remedies

The FCRA does not impose wholesale liability on the above-mentioned users of credit information. In most instances, actual damages and attorneys fees are available for violations.<sup>86</sup> However, under no circumstances can a consumer successfully seek injunctive relief, a right which is solely reserved for the FTC.<sup>87</sup> Considering the pain and heartache that ID theft causes, it offends the notions of justice that actual damages are the only true remedy

---

78. 15 U.S.C.S. § 1681s-2(a) (Lexis Nexis 2007).

79. 15 U.S.C.S. § 1681s-2(b).

80. 15 U.S.C.S. § 1681s-2(b)(1)(A-D).

81. *Whiseant v. First Nat'l Bank & Trust Co.*, 258 F. Supp. 2d 1312, 1316 (N.D. Okla. 2003).

82. *Nelson v. Chase Manhattan Mortg. Corp.*, 282 F.3d 1057, 1060 (9th Cir. 2002); *Roybal v. Equifax, Transunion, Experian Rickenbacker, Medamerica, City Towing Body Shop, Inc.*, 405 F. Supp. 2d 1177, 1179-1180 (E.D. Cal. 2005); *Cisneros v. Trans Union, L.L.C.*, 293 F. Supp. 2d 1167, 1174 (D. Haw. 2003).

83. *Alkagi v. Nationscredit Fin. Servs. Corp.*, 196 F. Supp. 2d 1186, 1192-93 (D. Kan. 2002).

84. *Stafford*, 262 F. Supp. 2d at 782.

85. *Peasley v. Verizon Wireless L.L.C.*, 364 F. Supp. 2d 1198, 1201 (S.D. Cal. 2005) (quoting *Nelson*, 282 F.3d at 1060).

86. 15 U.S.C.S. § 1681s(c)(1)(C) (Lexis Nexis 2007); see *Washington v. CSC Credit Servs.*, 199 F.3d 263, 269 (5th Cir. 2000); see also Bill would let ID theft victims seek restitution, Reuters, Oct. 17, 2007, available at <http://www.reuters.com/article/email/idUSN1619549220071017> (describing new legislation introduced in the Senate that could allow ID theft victims to seek monetary restitution from time spent navigating the financial red tape while attempting to restore their credit history.).

87. *Id.*

available to victims.<sup>88</sup>

For a true-name ID theft victim, FCRA's most disheartening burden lies in its seeming preemption of state remedies. A victim may sue for either willful or negligent violations of the enumerated duties<sup>89</sup> as long as they establish that the financial entities acted with malice<sup>90</sup> and the claim asserted is brought within two years of the date the claim arises.<sup>91</sup> Normally, when federal statutes do not provide comprehensive protection, individual states pass legislation aimed at "closing the gaps." For this particular injury, unfortunately, states are not permitted the authority to fill the gaps found in the FCRA.<sup>92</sup>

Two sections of the FCRA address state remedies. The first prohibits "the imposition of requirements or prohibitions by laws of any state with respect to any subject matter regulated" under § 1681s-2 in relation to the furnisher responsibilities.<sup>93</sup> Section 1681s-2 establishes guidelines for furnishing information to CRAs and addresses the duties of furnishers of information once they receive notice of a dispute.<sup>94</sup> The phrase "laws of any state" has been interpreted to refer to both statutory and common state law.<sup>95</sup> Thus, at first glance, it appears that all state laws are barred. Yet, FCRA also provides that "no consumer may bring any action or proceeding in the nature of defamation, invasion of privacy, or negligence with respect to the reporting of information against any [CRA], user of information, or [furnisher of information] . . . *except as to false information furnished with malice or willful intent to injure such consumer.*"<sup>96</sup> This suggests a plaintiff can establish a common law tort claim with respect to the reporting of information to CRAs if the plaintiff proves malice or willful intent to injure.<sup>97</sup> Because no federal appeals court "has provided guidance on these opposing preemption provisions,"<sup>98</sup> it is likely that a victim must prove malice or willful intent to cause injury in order to bring a successful state action claim.

#### **Identity Theft Penalty Enhancement Act of 2004**

Where FCRA concerns itself with the interplay between consumers and

---

88. *Jarrett*, 421 F. Supp. 2d at 1353.

89. 15 U.S.C.S. §§ 1681n, 1681o (Lexis Nexis 2007); see *Nagle v. Direct Merchs. Credit Card Bank, N.A.*, 2006 U.S. Dist. Lexis 29835, at \*2 (E.D. Pa. Mar 23, 2006).

90. 15 U.S.C.S. § 1681h(e) (Lexis Nexis 2007); see *Stafford*, 262 F. Supp. 2d at 782.

91. 15 U.S.C.S. § 1681p (LexisNexis 2007).

92. *Holtman v. Citifinancial Mortgage Co.*, No. 3:05-cv-1571, 2006 U.S. Dist. LEXIS 43730, \*8 (D. Conn. June 19, 2006).

93. 15 U.S.C.S. § 1681t(b)(1)(F) (LexisNexis 2007).

94. 15 U.S.C.S. § 1681s-2(a), (b) (LexisNexis 2007).

95. *Holtman*, 2006 U.S. Dist. LEXIS 43730, at \*8.

96. 15 U.S.C.S. 1681h(e) (LexisNexis 2007) (emphasis added).

97. *Rivera v. Countrywide Fin. Corp.*, No. 1:04CV103, 2006 U.S. Dist. LEXIS 59186, \*7 (S.D. Miss. August 21, 2006); *Alabran v. Capital One Bank*, No. 3:04CV935, 2005 WL 3338663, \*5 (E.D. Va. Dec. 8, 2005); *Watson v. Trans Union Credit Bureau*, No. Civ.04-205-B-C, 2005 WL 995687, \*6-8 (D. Me. Apr. 28, 2005).

98. *Rivera*, 2006 U.S. Dist. LEXIS 59186, at \*8.

America's credit gate-keepers, ITPEA more directly addresses the problem of ID theft.<sup>99</sup> Although intended primarily as a measure to combat terrorists' use of false identities, the act stiffens penalties for any ID thief.<sup>100</sup> Signed into law by President George W. Bush in 2004, ITPEA attempts to make ID theft punishment a better reflection of the pain associated with becoming an ID theft victim. As President Bush expressed, "too often, those convicted have been sentenced to little or no time in prison. This changes today."<sup>101</sup>

ITPEA created an enhanced criminal penalty for anyone who, while engaging in an enumerated felony,<sup>102</sup> "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person."<sup>103</sup> The term "means of identification" includes the personal data that thieves use to perpetrate identity fraud, such as another person's name or social security number.<sup>104</sup> Now mere possession of a means of identification with intent to

---

99. 18 U.S.C.S. § 1028A (LexisNexis 2007).

100. Tim Lemke, *Penalties Stiffened for Identity Theft*, THE WASHINGTON TIMES, July 16, 2004, at C11.

101. *Bush Signs Legislation Subjecting Identity Thieves to Tougher Penalties*, 9 Elec. Com. & L. Rep. (BNA) 636, 636 (July 21, 2004).

102. The felonies that give rise to additional liability under the ITPEA are those:

Relating to the theft of public money, property, or rewards in violation of 18 U.S.C.S § 641; Relating to the theft, embezzlement, or misapplication by bank officer or employee under 18 U.S.C.S § 656; Relating to theft from employee benefit plans in violation of 18 U.S.C.S § 664; Relating to false [im]personation of citizenship in violation of 18 U.S.C.S § 911; Relating to false statements in connection with the acquisition of a firearm in violation of 18 U.S.C.S § 922(a)(6) Provisions contained in this chapter (relating to fraud and false statements), other than this section or 18 U.S.C.S § 1028(a)(7); Relating to mail, bank, and wire fraud in violation of any provision contained in 18 U.S.C.S §§ 1341 et seq.; Relating to nationality and citizenship in violation of any provision contained in 18 U.S.C.S §§ 1421 et seq.; Relating to passports and visas in violation of any provision contained in 18 U.S.C.S §§ 1541 et seq.; Relating to obtaining customer information by false pretenses in violation of section 523 of the Gramm-Leach-Bliley Act (15 U.S.C. 6823); Relating to willfully failing to leave the United States after deportation and creating a counterfeit alien registration card in violation of section 243 or 266 of the Immigration and Nationality Act (8 U.S.C. 1253 and 1306); Relating to various immigration offenses in violation of any provision contained in chapter 8 of title II of the Immigration and Nationality Act (8 U.S.C. 1321 et seq.); or Relating to false statements relating to programs under the Act in violation of section 208, 811, 1107(b), 1128B(a), or 1632 of the Social Security Act (42 U.S.C. 408, 1011, 1307(b), 1320a-7b(a), and 1383a). 18 U.S.C. § 1028A(c). NOTE: under new legislation proposed in a bipartisan bill in the senate, use of "key loggers" and other spy ware could become a felony in of itself; if passed, it is possible that such use could become an additional enumerated felony in the near future. See Reuters, *Supra* note 86.

103. 18 U.S.C.S. § 1028A(a)(1); *see also* United States v. Godin, 476 F. Supp. 2d 1, 2 (D. Me. 2007).

104. *United States v. Hines*, 472 F.3d 1038, 1039 (8<sup>th</sup> Cir. 2007) citing 18 U.S.C. § 1028(d)(7)(A).

commit a crime is a crime in itself.<sup>105</sup> The purpose of this shift in policy, according to Chris Hoofnagle, Deputy Director of the Electronic Privacy Information Center in Washington, D.C., is to induce prosecutors to bring more ID theft cases.<sup>106</sup>

ITPEA achieves its intended goal by creating the crime of “aggravated identity theft,” which occurs when a thief utilizes a stolen identity to commit other crimes.<sup>107</sup> From a practical standpoint, ID theft is not a criminal end in itself, but a means to achieve some other illegal end. As a result, few identity thefts can now be classified as anything other than “aggravated”. Under this new statute, aggravated identity thieves are sentenced to an additional two years of prison time in addition to the sentences they receive if they are convicted of the underlying crimes committed using the misappropriated identity.<sup>108</sup> The aggravated sentences imposed by ITPEA are triggered only by the conviction of a felony enumerated in 1028A(c).<sup>109</sup> This subsection lists “the federal statutes that punish the crimes of larceny, embezzlement and generic fraud, in other words, the federal crimes most likely to be associated with identity theft.”<sup>110</sup> The minimum sentence under the statute is two years.<sup>111</sup>

One concern associated with this law is its imposition of “mandatory minimums.”<sup>112</sup> The language of the statute requires that: *any* knowing possession or use of the identity of another *will be sentenced* to an additional two-year prison term with no possibility of probation.<sup>113</sup> For some, mandatory minimums are concerning because they encumber judicial sentencing discretion.<sup>114</sup> Critics of mandatory minimums argue that judges are best suited to balance the needs of justice with the eccentricities of each case. For others (including the United States Congress), the loss of judicial discretion pales in comparison to the increased disincentive now thrust upon potential ID theft offenders.<sup>115</sup> Advocates of this approach look at a statutory framework clearly unequipped to deal with the tidal wave of criminal activity that is identity theft as their motivation for change. Only time will tell if this law will achieve its stated goals.

---

105. Robert E. Holtfreter & Kristy Holtfreter, Gauging the Effectiveness of US Identity Theft Legislation, 13 J. FIN. CRIME 56, 62 (2006), [http://www.fraudupdate.com/fsu/cn.nsf/369fe1f2c6e098818525711d00527bff/\\$FILE/IDTheftLegis.pdf](http://www.fraudupdate.com/fsu/cn.nsf/369fe1f2c6e098818525711d00527bff/$FILE/IDTheftLegis.pdf) (2006).

106. Declan McCullagh, *Season Over for 'Phishing'*, CNET NEWS.COM, July 15, 2004, [http://news.com.com/2100-1028\\_3-5270077.html](http://news.com.com/2100-1028_3-5270077.html).

107. 18 U.S.C.S. 1028A.

108. United States v. Jimenez, No. 05-10058-RGS, 2005 U.S. Dist. LEXIS 22407, \*1-2 (D. Mass. October 4, 2005).

109. *Id.* at \*4.

110. *Id.*

111. 18 U.S.C. 1028A.

112. McCullagh, *supra* note 106.

113. 18 U.S.C.S. 1028A(a)(1), (b)(1).

114. McCullagh, *supra* note 106.

115. *Id.*

In essence, the ITEPA's role in the fight against ID theft is to "beef up" the punishment for ID thieves through the creation of a new "aggravated" version of the crime. The traditional purpose of harsher prison sentences is to have a chilling effect on the amount of crime carried out. If the overall goal of the ITEPA is to decrease the amount of ID thefts committed, it fails to consider the basic concept of risk versus reward. As it stands, 99% of all ID thieves escape justice.<sup>116</sup> Recognizing that the average ID theft discovery takes place long after the fraud occurs, the risk of apprehension – and the imposition of an additional two-year prison sentence – is a minor deterrent when weighed against the potential windfall successful ID thieves typically receive. The imposition of harsher prison sentences may not be a bad idea, but its length must be calculated to actually deter future thefts from occurring.

### *International Efforts*

Online ID theft is not an offense perpetrated exclusively by American criminals. The Internet is a community without borders. At its core, the Internet is a mechanism for connecting multiple computers using a loose and largely ungoverned network.<sup>117</sup> Cyber crime can originate just as easily from your neighboring city as it can from across the world. An Australian criminal could steal the identity of a German citizen and use it to defraud an American bank. A thief can steal any person's identity and sell it to the highest bidder on the international black market.

American laws do not often concern criminals in foreign jurisdictions. Indeed, "countries where cyber crime flourishes tend to have weak laws dealing with computer crime, law enforcement agencies that lack computer forensic capabilities and an underdeveloped apparatus for collaborating with law enforcement agencies in other countries."<sup>118</sup> The Anti-Phishing Working Group estimates that more than 70% of phishing websites are hosted outside of the U.S.<sup>119</sup> China, for example, is now responsible for 11.96% of all worldwide phishing sites, and countries such as the Republic of Korea and Germany host many of the remaining sites.<sup>120</sup>

As the Internet further evolves into a global tool, online ID theft may become more prevalent and difficult to check. Some in the international

---

116. Zeller, *supra*, note 4.

117. Vinton G. Cerf, "First, Do No Harm", INTERNET GOVERNANCE: A GRAND COLLECTION, March 25-26, 2004, at 13-15, available at [www.unicttaskforce.org/perl/documents.pl?do=download;id=778](http://www.unicttaskforce.org/perl/documents.pl?do=download;id=778).

118. Robert Louis B. Stevenson, *Plugging the "Phishing" Hole: Legislation versus Technology*, 2005 DUKE L. & TECH. REV. 0006, ¶ 18 (2005) citing Thomas Fedorek, *Computers + Connectivity = New Opportunities for Criminals and Dilemmas for Investigators*, 76-FEB N.Y. St. B.J. 10, 16 (2004).

119. *Combined Report for September and October, 2006*, PHISHING ACTIVITY TRENDS REPORT (Anti-Phishing Working Group), Dec. 2006, at 5 available at [http://antiphishing.org/reports/apwg\\_report\\_september/october\\_2006.pdf](http://antiphishing.org/reports/apwg_report_september/october_2006.pdf).

120. *Id.*

community share the U.S.'s recognition that phishing and online fraud have disastrous consequences for the entire world.

### The European Union

In 1995, the European Union approved the Data Privacy Directive (“the Directive”), a comprehensive declaration calling for protection of individuals in the collection and use of personal data.<sup>121</sup> The Directive was implemented to “protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.”<sup>122</sup> European Union member states are directed to adopt privacy-in-information laws *sui generis*, subject to general policy goals and certain minimum standards.<sup>123</sup>

One way in which the Directive is more proactive than American laws is in its application. Whereas American laws focus primarily on public furnishers of information and CRA's, the EU mandate “covers any use of personally identifiable information for any purpose.”<sup>124</sup> For example, the Directive requires specific approval “for any [online] use of [personal] data for any reason,”<sup>125</sup> and only permits use of personal data after “the data subject has consented unambiguously.”<sup>126</sup> It is undeniable that this method of enforcement is more comprehensive than the American approach. From a victim's viewpoint, blanket imposition of privacy-in-information prevents the occurrence of more ID thefts. The Directive also provides more avenues for restitution from the thefts that do occur. Moreover, the Directive deals with the particular hardship associated with online ID theft by mandating “common standards for transfers of information to third countries.”<sup>127</sup> As commentators have noted, however, the Directive contains numerous legal “loopholes.”<sup>128</sup> One such loophole is that it applies only to natural persons and not to legal

---

121. Council Directive 95/46/EC, art. 1, 1995 O.J. (L. 281/38) (EU). *Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/95-46-ce/dir1995-46\\_part1\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf) (Oct. 24, 1995).

122. *Id.*

123. Pamela Samuelson, *Five Challenges for Regulating the Global Information Society* 5, [http://www.ischool.berkeley.edu/~pam/papers/5challenges\\_feb22\\_v2\\_final\\_.pdf](http://www.ischool.berkeley.edu/~pam/papers/5challenges_feb22_v2_final_.pdf) (last visited Apr. 16, 2007).

124. Steven Andersen, *Six E-Commerce Pitfalls And How to Avoid Them*, Corporate Legal Times (Sept. 2000) (available in LEXIS, News Library); See generally Nicole M. Buba, Student Author, *Waging War Against Identity Theft: Should the United States Borrow From the European Union's Battalion?*, 23 Suffolk Transnat'l L. Rev. 633, 655 (2000).

125. *Id.* at Andersen.

126. Diane K. Bowers, *Privacy Online*, Marketing Research: A Magazine of Management & Applications (Fall, 1997) (available in LEXIS, News Library).

127. Buba, *supra*. n. 124 at 655 (citing Spiros Simitis, *From the General Rules on Data Protection to a Specific Regulation of the Use of Employee Data: Policies and Constraints of the European Union*, 19 Comp. Lab. & Pol'y. J., 351, 352-353 (1998)).

128. Patrick J. Murray, *The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet this Standard?*, 21 Fordham Int'l L.J. 932, 960 (1998).

entities.<sup>129</sup> These loopholes make it possible for users of personal data to avoid full compliance or liability.

In late November of 2001, thirty countries<sup>130</sup> comprising the Council of Europe Convention on Cybercrime, having recognized “the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies,”<sup>131</sup> passed the first international treaty (the “Treaty”) to deal explicitly with Internet-based crime.<sup>132</sup> Like the Directive, the Treaty sets forth minimum standards through which ratifying countries should create laws to prevent and prosecute cybercrime.<sup>133</sup> Specifically, ratifying countries are instructed to criminalize illegal access to computer systems and data, illegal interception of data, and the domestic use of a computer in the commission of an international fraud.<sup>134</sup>

The Treaty’s chief advantage is the uniform way in which members prosecute cyber criminals. In the past, criminals could conduct international ID theft from countries where the domestic fraud penalties were relaxed. Furthermore, the Treaty cedes prosecutorial jurisdiction of any cyber crime to the State in which the crime was committed, or “by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.”<sup>135</sup> Ratifying nations must also allow for the cross-border collection and use of “informational data” in investigations and prosecutions.<sup>136</sup> Although the United States became a signatory to the Treaty in 2003<sup>137</sup>, it has not yet been ratified by the Senate.<sup>138</sup>

### Canada

In many respects, the U.S. and Canada employ similar methods to combat online ID theft. For example, as in the United States, Canadian users of information are self-policing and much of the country’s regulations focus on furnishers of personal data.<sup>139</sup> Unlike the United States, however, Canada has established the Model Code for the Protection of Personal Information (“the

---

129. *Id.*

130. Dept. of Justice, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cybercrime*, <http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm> (last updated, Nov. 10, 2003).

131. *Convention on Cyber crime* preamble (Nov. 23, 2001), <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm>.

132. Lauren L. Sullins, Comment, “Phishing” for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft, 20 EMORY INT’L L. REV. 397, 420 (2006).

133. *Convention on Cybercrime*, *supra* note 148, at art. 2.

134. *Id.* at arts. 2,3,6 & 8

135. *Id.* at art. 22.

136. *Id.* at arts. 16-21.

137. Dept. of Justice, *supra*, note 130.

138. Sullins, *supra* note 132, at 421.

139. Jonathan P. Cody, Comment, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self Regulation?*, 48 CATH. U.L. REV. 1183, 1215 (1999).

“Code”), a national effort designed to provide personal information security.<sup>140</sup> Applied to all Canadian organizations that collect or use personal data, the Code sets forth ten specific performance principles in an attempt to balance the privacy rights of individuals and the information requirements of private organizations.<sup>141</sup> Key principles are codified in Canada’s Personal Information Protection and Electronic Documents Act.<sup>142</sup>

The two most significant principals advocated in the Code are accountability and consent. Unlike the U.S., all Canadian users of personal data are wholly accountable for its management.<sup>143</sup> For example, a neighborhood grocery store is just as liable for personal data losses as a national bank. Under the American method, by contrast, banks and credit agencies are the primary holders of liability, and only under the special circumstances noted above. Broad legal responsibility applies to all links in the personal data use chain promotes attentiveness on the part of personal data custodians. The Canadian method also requires that the individual have knowledge and provide consent before any collection, use, or disclosure of personal information is made, except where legal, medical, or security concerns makes such consent impractical.<sup>144</sup> Essentially, the Code creates in all users of personally identifiable information a new affirmative duty: the duty of approval. If each consumer must give her consent before an information user discloses data, the frequency of fraudulent disclosures will shrink. Like the tort claims that may be brought under the FCRA, the fraudulent disclosures that do occur can form the basis for negligence. The approval duty also means that more ID theft victims have the opportunity to receive punitive damages.

In essence, both the European and Canadian methods encourage the prevention of ID theft by creating more avenues for victims to receive punitive damages. To the extent that tort liability is increased, fewer consumers are exposed to victimization. As for those who are made victims, like those of violent crimes, fraud victims are not “made whole” upon receipt of punitive damages. These damages imply recognition that ID theft is a horrifying ordeal in a way that actual damages never could.

### PART III: SOLUTIONS

If the situation looks bleak, it should. Current federal and state statutes fall short because they are designed to protect credit providers and promote consumer confidence, rather than to compensate the true victims of ID theft.

---

140. Stephanie Byers, Note, *The Internet: Privacy Lost Identities Stolen*, 40 BRANDEIS L.J. 141,158 (2001).

141. The Canadian Standards Association, *About the Privacy Code*, <http://www.csa.ca/standards/privacy/code/Default.asp?language=English> (Last Visited March, 1996).

142. *Id.*

143. *Id.* at Principle 1.

144. *Id.* at Principle 3.

As shown above, too many victims' claims, especially those frauds occurring internationally, fall outside the scope of the ITPEA's and FCRA's coverage, and the majority of state remedies have been preempted by the FCRA. The manner in which the American legal system deals with ID theft is its fundamental flaw: punishment provides little comfort to those already victimized. Deterrence, on the other hand, through prevention, circumvents the deep trauma ID theft victims experience, and has the added benefit of eliminating the burden on an already over-stressed judicial system.

Below, I propose a few ways to achieve true-identity security by focusing on preventing the problem rather than punishing the offenders. It should be noted that, regardless of whether a thief goes online or stays in the "real world," one common thread seems to connect every ID theft: at some point, a thief's impersonation deceives a financial institution, government entity, service provider, merchant, or individual. Deterrence must be focused upon this critical juncture.

#### ***Tradable Credit System – a free market solution***

Congress should authorize the creation of a tradable credit system for all commercial institutions and merchants who utilize personal consumer data, making ID theft solutions the responsibility of all governmental and commercial users of personal data, rather than the responsibility of only Congress or victims.

A tradable credit system is one whereby a regulatory agency identifies and places a threshold level of "acceptable failure" on all significant users of personal consumer data. For the purposes of this paper, "acceptable failure" is the upper limit of negative behavior allowable under the law. The agency then allocates a number of time-fixed allowances or credits consistent with that limit. Commercial entities are then given the freedom to purchase new credits in an open market for the right to engage in additional "failure" activities and to sell credits unused due to better-than-required security practices.<sup>145</sup>

As a method of monitoring the credit use, a specified agency would assign a point system that contemplates different ways through which private organizations stay within or exceed the boundaries of "acceptable failure." By way of illustration, consider the automobile speeding ticket system. Different speeding offenses are assigned point levels, the most severe of which have higher point values. Over time, the points accrue and approach an unacceptable level as determined by the Department of Motor Vehicles. There are intermediate penalties throughout the process – fines and "traffic school" for example. When a driver accumulates too many points, her license is suspended and revoked. Criminal charges can then be imposed as a penalty for

---

145. See Donald F. Larson & Paul Parks, *Risks, Lessons Learned and Secondary Markets for Greenhouse Gas Reductions* 3, 49-50, <http://www.worldbank.org/html/dec/Publications/Workpapers/wps2000series/wps2090/wps2090.pdf> (last visited Apr. 16, 2007).

operating a motor vehicle without a valid license. The same principles will well when applied to a tradable credit system.

Any private organization utilizing, benefiting from, or collecting personal consumer data would be subject to the credit trading system enforced by the FTC. The FTC is the logical choice for regulatory oversight. It is the regulatory body in charge of overseeing enforcement of the FCRA, and therefore it is already experienced in the supervision of personally identifiable data. Due to the widespread use of credit and personal data, a successful solution to ID theft is only possible through broad participation. Financial institutions<sup>146</sup> and utility companies are obvious examples of data users, but everyone from mobile phone companies<sup>147</sup> to department stores and Internet service providers require and store personal data. These organizations are informational “gate-keepers;” the proverbial front line of fraud prevention. It is time for business perspectives to change – utilization of credit and personal information is a privilege and not a right; responsibility must be synonymous with use.

This solution is not novel; it is already successfully used to cut corporate greenhouse emissions. In 1970, Congress passed the Clean Air Act (the “CAA”),<sup>148</sup> launching ambitious objectives for improving the U.S.’s air quality. Since the 1977 amendments,<sup>149</sup> the Environmental Protection Agency (the “EPA”) has been “developing and implementing a variety of market-based programs aimed at achieving the Act’s objectives.”<sup>150</sup> For example, through the power of open markets, the EPA was successful in phasing out lead from gasoline.<sup>151</sup> Urban areas have implemented Tradable Development Right (“TDR”) programs to protect open space, landmarks, and other sensitive areas.<sup>152</sup> New Jersey has been able to limit development in the Pinelands forest zone through a widely publicized TDR scheme.<sup>153</sup> If properly established, tradable credit systems are proven to be a positive source of social change and can succeed in the area of identity theft.<sup>154</sup>

Tradable credit systems can provide mutual benefits to all parties involved. By making users of personal data responsible for prevention, the American public immediately benefits from fewer and less severe ID thefts. At the same time, businesses have the opportunity to generate new streams of revenue. Organizations who out-perform the agency-mandated ceiling can

---

146. *Jarrett*, 421 F. Supp. 2d at 1351.

147. *Peasley*, 364 F. Supp. 2d at 1198.

148. 42 U.S.C. §§ 7401-7671(q) (2000).

149. *Id.*

150. David Sohn & Madeline Cohen, Note, *From Smokestacks to Species: Extending the Tradable Permit Approach from Air Pollution to Habitat Conservation*, 15 STAN. ENVTL. L.J. 405, 416 (1996).

151. Larson & Parks, *supra* note 162, at 10.

152. Sohn & Cohn, *supra*, note 150, at 410-411.

153. *Id.*

154. Vivien Foster & Robert W. Hahn, *Designing More Efficient Markets: Lessons from Los Angeles Smog Control*, 38 J.L. & ECON. 19, 21 (1994).

utilize unused credits as a commodity to be sold on the open market. Signatories to the Kyoto protocol, an international treaty devoted to the “stabilization of greenhouse gas concentrations in the atmosphere”<sup>155</sup> established a carbon reduction credit-trading system similar to the one that resulted from the U.S.’s Clean Air Act.<sup>156</sup> In early March of 2006, Endesa, Spain’s largest power company, announced plans to purchase carbon credits from the China Huaneng Group (CHG) (the “CHG”), China’s biggest power producer.<sup>157</sup> In various ways, the CHG invested in cleaner sources of energy with the goal of selling their carbon credits.<sup>158</sup> The CHG’s reward totaled \$36 million.<sup>159</sup> Imagine how thoroughly personal data will be protected when businesses discover that a secure system can generate profit.

Critics might argue that smaller businesses will face too high of a burden in the form of increased costs. Because small businesses are privately capitalized and expenses are often tightly controlled, the argument is that there is little room in the budget to devote to the creation of new data security practices. As is the case here, however, all marketable rights based solutions can mitigate initial adoption costs through at least two ways. First, businesses that adopt superior security measures can sell unused personal data credits. These funds can easily be applied to alleviate the costs of adoption. Second, the costs associated with creating a security system are non-recurring capital expenditures that would qualify for normal amortization and depreciation.<sup>160</sup> As a result, costs associated with implementation of new security practices can be offset by a reduced tax burden. It should also be noted that the system works best when individual entities are given the freedom to generate their own processes for securing personal data. For example, suppose there are three levels of data security: maximum, average, and minimal. Naturally, all three levels have potential risk and reward depending on individual cost and efficiency. Each individual business is free to select a level that is most appropriate based on its own criteria. The market will then reward or punish the business for its choices. This method allows each business to choose its own security burden, making it as least obtrusive as possible. It also creates thousands of “little laboratories,” in an effort to create the most efficient and effective security practices through nation-wide trial and error. As successful and inferior security techniques are refined over time, the U.S.’s greatest minds will find the best solution in a way that is uncorrupted by the political system and driven by a powerful motivator: the prospect of higher profits. Few other

---

155. The United Nations Framework Convention on Climate Change, *Convention on Climate Change* art. 2, [http://unfccc.int/essential\\_background/convention/background/items/1353.php](http://unfccc.int/essential_background/convention/background/items/1353.php) (Mar. 21, 1994).

156. Wang Ying, *Profit Power*, CHINA DAILY, Mar. 6, 2006, [http://chinadaily.com.cn/english/doc/2006-03/06/content\\_526875.htm](http://chinadaily.com.cn/english/doc/2006-03/06/content_526875.htm).

157. *Id.*

158. *Id.*

159. *Id.*

160. MSN Money, *Glossary of Terms*, <http://moneycentral.msn.com/taxes/glossary/glossary.asp?TermID=49>

solutions are so positively driven.

For this system to function properly, security breaches must be matched with credit usage in each end-of-accounting period. The FTC will have to play an active role in ensuring compliance with credit usage standards. Assume, for example, that a thief hacks into the mainframe database of a major credit card company and steals the personal data of 10,000 customers. Surely, the company will not have enough failure credits for this extreme level of security breakdown. By the end of the next accounting period, the company must purchase enough credits to offset the points it has accrued due to the security breach. Failure to do so should result in the imposition of criminal charges and/or punitive fines by the FTC; moneys used to help fund the cost of enforcement, in addition to the actual damages to the victim for willful violation of standards.

In theory, “marketable rights systems offer a powerful means” for achieving any security-related goal.<sup>161</sup> They establish mechanisms for assessing competing “good” and “bad” policy values, for example “secure” and “insecure” methods for dealing in personal data.<sup>162</sup> To achieve success, trading systems must include processes for: delineating the type of organization bound under the system; determining the upper limit of an “acceptable failure”; “evaluating point values associated with different levels of security failure and assigning credits to data users; trading in personal data credits on an open market; and securing performance, i.e., guaranteeing compliance with requirements and security objectives.<sup>163</sup>

Everyday, we rely on the aggregate creativity of American business people to improve our quality of life. Business people, concerned primarily with the bottom line, are in the unique position to eliminate ID theft by circumventing the practices that lead to fraud. By implication, prevention as a concept recognizes and accounts for the burden that ID theft places on victims in a way that mere management never could.

### ***Technology***

ID theft is an unpreventable problem as long as identity verification relies upon words and numbers. Although the market-based solution outlined above can make tangible differences in the lives of the American public, some ID thefts will inevitably still occur. The future of ID theft protection, therefore, is in technology. Bioverification, technology that utilizes genetic make-up as a method of identity verification, has the potential to become a powerful form of

---

161. Sohn & Cohn, *supra*, note 150, at 410.

162. Sohn & Cohn, *supra* note 150, at 410.

163. See Sohn & Cohn, *supra* note 150, at 412. (citing Jon H. Goldstein & Theodore Heintz, Jr., *Incentives for Private Conservation of Species and Habit: An Economic Perspective*, in BUILDING ECONOMIC INCENTIVES INTO THE ENDANGERED SPECIES ACT 51, 55 (Wendy E. Hudson ed., 1994)).

fraud protection.<sup>164</sup> Congress must monetarily encourage, whether through direct subsidization or tax incentives, widespread adoption of bioverification systems.

### **Fingerprint Identification Technology**

Fingerprinting is a branch of forensic science that differentiates between the distinctive patterns of ridges and valleys that flow across fingertips.<sup>165</sup> These ridges and valleys are formed while in the womb and are the product of a matchless combination of hereditary and environmental factors.<sup>166</sup> Fingerprints are statistically unique and never change.<sup>167</sup> For decades, forensic scientists used the Henry system to manually distinguish between billions of known prints using three basic fingerprint patterns: arch, loop, and whorl.<sup>168</sup> Today the process is predominantly computerized<sup>169</sup> and therefore, fingerprinting is an ideal identity verification method.<sup>170</sup>

The fingerprint identification process functions when “a fingerprint of unknown ownership is matched against a database of unknown fingerprints to associate a crime with an identity”.<sup>171</sup> Thus, a person’s identity is verifiable upon comparison of two sets of fingerprints; one set stored and previously matched to the individual, and another set offered at the time of verification. An individual’s identity is verified by computer when the two sets of prints are a statistical match.

The use of fingerprints as an identification device is already in wide circulation, primarily as a law enforcement tool and for registration of aliens with Citizenship and Immigration Services (formerly the Immigration and Naturalization Service). The recent presence of certain factors makes this technology realistically adaptable for wide spread commercial use.<sup>172</sup> These factors include “small and inexpensive fingerprint capture devices, fast computing hardware, recognition rate and speed to meet the needs of many applications, the explosive growth of network and Internet transactions, and

---

164. Lawrence O’Gorman, *Fingerprint Verification*, in *Biometrics: Personal Identification in Networked Society* 43, 45 (Anil K. Jain, Ruud M. Bolle, & Sharath Pankanti eds., 1999).

165. Matthew McClearn, *Canadian Business, Technology, Tale of Gun*, (Feb. 26, 2007) (available in LEXIS, News Library).

166. O’Gorman, *supra* note 164, at 46.

167. McClearn, *supra* note 165.

168. *See generally* Edward R. Henry, CLASSIFICATION AND USES OF FINGER PRINTS (George Rutledge & Sons, Ltd. 1900), available at <http://www.clpex.com/Information/Pioneers/henry-classification.pdf>.

169. Sung Bum Pan ET AL., *A Memory-Efficient Fingerprint Verification Algorithm Using a Multi-Resolution Accumulator Array*, 25 ETRI J. 179, 179 (2003), available at <http://etrij.etri.re.kr/Cyber/servlet/GetFile?Fileid=SPF-1055456865372>.

170. Government Computer News, *Is it Live, or is it...Latex?*, GOV’T COMPUTER NEWS, Aug. 15, 2005, available at LEXIS (the newer generation of fingerprint readers scan a “complex structure of collagen and blood vessels” below the surface of the finger in order to increase security).

171. O’Gorman, *supra* note 164, at 45.

172. Bum Pan ET AL., *supra* note 169, at 185.

the heightened awareness of the need for ease-of-use as an essential component of reliable security.”<sup>173</sup>

### **Retinal Scan Identification Technology**

A Retinal Scan photographs the inside of the human eye for the purpose of identity verification. The scan studies the layer of blood vessels located in the back of the eye using a “low-intensity light source and an optical coupler and can read . . . patterns at a great level of accuracy.”<sup>174</sup> The eye has unique characteristics that make a scan reliable, long lasting, and difficult to counterfeit.<sup>175</sup> For example, the eye does not change between birth and death,<sup>176</sup> and because the retina is located inside of the eye, it is protected from variations “caused by exposure to the external environment.”<sup>177</sup> Just like fingerprints, retinal scan technology verifies an individual’s identity by comparing a current digital image of the retina with one previously filed and stored.<sup>178</sup> Hundreds of distinctive ocular characteristics are quantified in a retinal scan in order to identify an individual.<sup>179</sup> Because of its high cost, it is predominantly used in “high security government installations,” including nuclear research sites and military bases.<sup>180</sup>

### **Use of Biometrics**

The elimination of human error is the most striking advantage of both methods. The current system of identify verification relies upon disclosure of numerous pieces of personal information.<sup>181</sup> Frequently, the system breaks down when a verifying employee fails to notice discrepancies contained in personal data offered by a thief. For example in *Stafford v. Cross Country Bank*, the thief obtained a credit card in the victim’s name by correctly listing the victim’s social security number and mother’s maiden name, but listing an incorrect home address,<sup>182</sup> and in *Patrick v. Union State Bank*, despite an inability to provide a home address, social security number, or even a full signature, a lost driver’s license was enough to open a checking account in the victim’s name.<sup>183</sup> Bioverification would protect identity integrity if it were used before extensions of credit and cashless transactions occur. In the future, social security and credit card numbers may even become obsolete in a world where bioverification is broadly implemented. A unique retinal make up can become a social security card number, credit card number, bank account

---

173. O’Gorman, *supra* note 164, at 43.

174. National Center for State Courts, *Individual Biometrics, Retinal Scan, Basics*, <http://ctl.ncsc.dni.us/biomet%20web/BMRetinal.html#basics> (last accessed, Apr. 16, 2007).

175. Robert “Buzz” Hill, *Retina Identification*, in *Biometrics: Personal Identification in Networked Society* 123, 123-24 (Anil K. Jain, Ruud M. Bolle, & Sharath Pankanti eds., 1999).

176. National Center for State Courts, *supra*, note 174, at Evaluation.

177. Hill, *supra* note 175, at 124.

178. *Id.* at 136.

179. *Id.*

180. *Id.* at 123-124.

181. Nauman, *supra* note 14.

182. *Stafford v. Cross Country Bank*, 262 F. Supp. 2d 776, 779-80 (W.D.Ky. 2003).

183. *Patrick v. Union State Bank*, 681 So.2d 1364, 1365 (Ala. 1996).

number, and driver's license all rolled up into one secure instrument. Without access to this information, identity thieves will have nothing to left to steal.

The key to biometric success is widespread adoption. Consumers must be able to present themselves for verification conveniently and quickly. As with credit card sliders, fingerprint and/or retinal scanners must be available for use in financial institutions and at all points of sale. Critics might argue that this method will stifle the use of the Internet to conduct commercial transactions because consumers cannot be expected to make the effort to purchase these scanners for in-home use and the elimination of credit card numbers would injure the relatively new medium. However, this point of view fails to take into account two important factors. First, the Internet is a marketplace that will be used for many decades to come. Consumers treasure e-commerce because thousands of merchants and products are available with just the click of a mouse. However, e-commerce can reasonably be expected to adapt to whatever security measures are thrust upon it. Second, and most important, consumers will probably not have to purchase the scanners, at least not explicitly. The scanners could become integrated into personal computers and laptops. IBM already sells biometric scanners built into its laptops as a security measure.<sup>184</sup> Whereas add-on security devices could reach prices up to \$200 just two years ago,<sup>185</sup> a modern integrated biometric scanner can cost just \$30, or 2.5% of a \$1,168 laptop.<sup>186</sup> Weighed against the financial and emotional costs associated with a stolen identity, \$30 for total identity security is a bargain.

Furthermore, biometrics is not the enemy of privacy that critics make it out to be. Their argument goes something like this: use of biometrics requires a large centrally controlled database that might be misused by those entities entrusted to act as custodians. Proponents of this viewpoint fear that if centrally stored, digital fingerprints or retinal scans might be subject to electronic monitoring and surveillance. Luckily, use of biometrics for identity security does not contemplate any central storage of data. Simply, encrypted biometric data would be stored on the credit card and function as a "lock." The card (and its corresponding bank account) could be "unlocked" and used for purchases as long as the individual presenting the card can verify her identity by matching the stored fingerprint or retinal scan. Verification would then be a straightforward procedure. Either the scan would present a match with what was scored or it does not; the card could only function with a match. Because no third party, including the cashier, would have access to the

---

184. Akira Hino & Stacy Cannady, *Integrated Fingerprint Reader*, 5-10, [http://www.pc.ibm.com.us/pdf/fingerprint\\_Reader\\_white\\_paper.pdf](http://www.pc.ibm.com.us/pdf/fingerprint_Reader_white_paper.pdf) (2004).

185. Jack M. Germain, *IBM Introducing Fingerprint Reader into Laptop*, TECHNEWSWORLD, Oct. 4, 2004, <http://technewsworld.com/story/37017.html>.

186. IBM, *Lenovo Thinkpad T60 WideScreen*, <http://www.shop.lenovo.com/SEUILibrary/controller/catalog.workflow:category.detail?current-catalog-id=12F0696583E04D86B9B79B0FEC01C087&current-cataegory-id=3FD8C234713A440BA8062AAEBCA813BF> (last visited Apr. 16, 2007).

biometric data, it could not be misused. This technology is already being utilized. Walt Disney World uses finger scans to match visitors to their admission passes,<sup>187</sup> and in the wake of the terrorist attacks on September 11, 2001, admittance to the Statue of Liberty in New York is conditioned upon leaving bags and recording equipment in lockers that can only be accessed with fingerprints.<sup>188</sup> ATM cash machines and debit cards operate in a similar fashion. Both rely upon two layers of security: a physical card and a secure password for account access. Instead of a pin number, the second layer of security here is a biometric scan.

Despite its potential to change the way the U.S. deals in cashless transactions, bioverification technology will take many years to become widely adopted if left on its own. Too many variables may stall or divert its ability to protect the American people from identity-related frauds. Although the technology exists and is reliable, it is still comparatively expensive. Investment must be made in mass production to bring bioverification to the forefront of the war on ID theft. To implement a change, Congress must support investment through bioverification incentives.

### CONCLUSION

For better or for worse, we are a society that relies primarily upon cashless transactions. We use credit for everything from securing a bank loan to purchasing new jeans. It has become a part of the fabric of our culture. While the threat of fraud was always present, the digital age has made deception alarmingly sophisticated. The explosion of Internet use attracts sharks that prey mercilessly on victims. Thieves count on consumer naiveté and organizational red tape to screen their disappearance. Although some positive steps have been taken by Congress, current remedies do nothing to assuage the most potent sting of ID theft; its emotional impact.

Both solutions explored in this article focus on prevention of ID theft and the practicality of implementation. Through implementation of the market-driven solution, a decrease in the number and severity of ID thefts could correspond with more robust revenue streams for businesses. Whereas current Congressional solutions seek to limit liability expansion only to a select class under narrow circumstances, this approach attempts to encourage the creation of tighter security procedures through incentives. The second solution recognizes that Congress is in a unique position to be the “spark” that is necessary to propagate a technological solution to the ID theft problem. Although each solution can be effective on its own, if adopted in unison, the two can be synergistic.

---

187. Jennifer Peltz, *Scanning Hands and Eyes to Verify ID for Access and Payroll is a Growth Industry, but it Troubles Some; a new Body of Work*, *NEWSDAY*, Aug. 15, 2006, at A41, available at LEXIS.

188. Peter Callaghan, *Some Chilling Moments at Florida Theme Parks come before any of the Rides*, *THE NEWS TRIB.* (Tacoma, Wash.), July 26, 2005, at B01, available at LEXIS.