IDENTITY THEFT IN CYBERSPACE: CRIME CONTROL METHODS AND THEIR EFFECTIVENESS IN COMBATING PHISHING ATTACKS

By Jennifer Lynch

> Dear Paypal valued member, It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems. However, failure to update your records will result in account suspension Please follow the link below and login to your account and renew your account information . . . .[1]

The above communication may appear, at first glance, to be a legitimate request from PayPal to update the accountholder's information. Instead, this e-mail is an example of the most recent form of identity fraud occurring on the Internet—"phishing."[2]

In the most common phishing scam, the "phisher" sends an e-mail disguised to look like it is from a financial institution or e-commerce site.[3] To appear credible and to attract the recipient's attention, the e-mail uses the company's logos and trademarks and employs "scare tactics" such as threats of account closure. The phishing e-mail typically tells the recipient she needs to update her account information "to avoid fraud" or for "security reasons" and directs her, through a link in the e-mail, to a fake site de-

---

1. I received this e-mail, conveniently, while working on this Note. It is reprinted exactly as I received it and includes the e-mail's punctuation and grammatical errors, which were much less glaring when viewed in the context of PayPal's logos and design. This e-mail made it through two spam filters, and caught my attention because I am a PayPal account holder.

2. The word "phishing" comes from an analogy to fishing; the e-mail is bait used to lure in "fish" from the "sea" of Internet users. The "f" is changed to "ph" in keeping with computer hacking tradition. Anita Ramasastry, *Hooking Phishermen*, CNN.COM, Aug. 16, 2004, *at* http://www.cnn.com/2004/LAW/08/16/ramasastry.phishing.

3. Although phishers generally use the guise of banks and retailers as "bait," recent phishing scams used the lure of donating to the John Kerry presidential campaign and the chance to buy an advance electronic copy of an upcoming Harry Potter book. *See* John Borland, *Con Artists 'Phish' for Campaign Donors*, CNET NEWS.COM, Aug. 3, 2004, *at* http://news.com.com/Con+artists+'phish'+for+campaign+donors/2100-1028_3-5295764.html; Lawrence Van Gelder, *J.K. Rowling Warns Fans*, N.Y. TIMES, Feb. 3, 2005, at E2.

signed to look exactly like the site of the business mentioned in the e-mail.[4] Once there, she is asked to enter her personal information and update her password. However, if she does, this information will be used not to "update" her account, but to steal her identity.

The terms "identity theft" and "identity fraud" describe the theft for fraudulent purposes of personal information, such as account numbers, social security numbers (SSNs), and other personal identifiers such as a mother's maiden name.[5] Victims of identity theft and phishing attacks primarily suffer financial losses. However, these crimes also exact a price on the victim in time and money spent trying to rebuild her credit and good name, and a price on society in business losses, generally passed on to consumers through higher costs for goods and credit. Phishing imposes an additional societal cost—loss of consumer confidence in conducting business online.[6]

---

4. Ramasastry, *supra* note 2; *see also* Internet Fraud Complaint Center, *'Spoofed' E-Mails & Websites—A Gateway to Identity Theft and Credit Card Fraud* 2 (2002) [hereinafter IFCC Intelligence Note], *at* http://www1.ifccfbi.gov/strategy/63003SpoofNote.pdf.

5. Most people define "identity theft" as the theft of personal identifying information for some kind of fraudulent purpose. However, some qualify this definition in two different ways. First, some limit identity theft to the theft of non-account information such as a social security number, driver's license number, or date of birth. *See e.g.*, 18 U.S.C.S. § 1028(d)(7) (LEXIS Supp. 2004); IDENTITY THEFT at vii (Claudia L. Hayward ed., 2004). Others may use a broader definition of identifying information to include the information just listed as well as account numbers, PINs, mother's maiden name, etc., but may limit the purpose of use to financial crimes such as account-takeovers or fraudulent account applications. *See* Richard M. Stana, *Identity Theft: Prevalence and Cost Appear to be Growing*, *in* IDENTITY THEFT, *supra*, 17, 49 [hereinafter Stana, *Identity Theft: Prevalence and Cost*]. This Note will use the broadest definition of identity theft; as such it will include the theft of any type of personal identifying information used for any purpose. However, the primary focus will be on the theft of personal information used for financial fraud, because this is the most common outcome of phishing attacks.

6. *See Introduction of the "Anti-Phishing Act Of 2004"*, 150 CONG. REC. S7897 (July 9, 2004) [hereinafter Senator Leahy Statement] (statement of Sen. Leahy), *available at* http://leahy.senate.gov/press/200407/070904c.html; *see also* Bob Tedeschi, *E-Commerce Report; Growing Concern About Fraud is Pushing the Online World into Action. The Task Looms Large, Though.*, N.Y. TIMES, Sept. 8, 2003, at C9 (discussing a 2003 Forrester Research poll of 39,000 Internet users that found that almost one-third were pessimistic about security on the Internet—the highest figure since the company began taking the poll in 1998). Tedeschi also quoted a Nielsen NetRatings Analyst who believes online retailers have lost "billions" due to customer wariness of buying online. Another recent article quoted an Internet-based security firm as stating that 29% of its survey respondents would avoid online shopping during the Christmas 2004 season due to e-mail scams. Bob Sullivan, *'Tis the Season for Phishing Scams*, MSNBC.COM, Nov.

This Note discusses the growing identity theft problem in cyberspace, focusing specifically on phishing attacks. Part I presents an overview of identity theft through a discussion of associated costs, laws, and stakeholders. Part II provides facts and statistics on the phishing problem. Part III sets up a structure for analyzing identity theft crime control methods based on primary, secondary, and tertiary responses to crime. The primary level includes victim self-help measures, the secondary level involves private-party architecture solutions, and the tertiary level includes public law enforcement efforts. Part III then discusses recent developments in fighting identity theft at each level, focusing on new laws and services that help consumers secure their identity, advances in private-party methods to detect and prevent fraud, and new and proposed changes to criminal laws used in the battle against identity theft. It also discusses the effectiveness of these new developments on phishing attacks, and critically examines who is best equipped to combat the phishing problem. The Note concludes that no single crime control method alone will be enough to combat phishing. Only a combined approach, incorporating strategies from each level, will diminish the phishing problem.

I. OVERVIEW OF THE IDENTITY THEFT PROBLEM IN THE DIGITAL AGE

Identity theft is one of the fastest growing crimes in the United States. A broad survey commissioned by the Federal Trade Commission (FTC) in September 2003, estimated that 9.9 million Americans had had their personal information stolen in the prior year,[7] collectively costing businesses $47.6 billion and consumers $5.0 billion.[8] The FTC Identity Theft Survey

---

24, 2004 (citing a survey conducted by MailFrontier, Inc.), *at* http://www.msnbc.msn.com/id/6560652.

7. FED. TRADE COMM'N, IDENTITY THEFT SURVEY REPORT 7 (2003) [hereinafter FTC SURVEY REPORT], *at* http://www.ftc.gov/os/2003/09/synovatereport.pdf. The FTC estimated these figures by extrapolating from the percentage of survey respondents who stated they had had their identity stolen. *Id.* at 3. This figure is much higher than previously expected. Based on self-reporting figures at private and federal consumer protection agencies, many thought, prior to this report, that the number of victims of identity theft was closer to 750,000. Timothy L. O'Brien, *Identity Theft Is Epidemic. Can It Be Stopped?*, N.Y.TIMES, Oct. 24, 2004, § 3 (SundayBusiness), at 1 (quoting the executive director at the consumer advocacy group Identity Theft Resource Center); *see also* Stana, *Identity Theft: Prevalence and Cost*, *supra* note 5, at 19 (noting that as of 2002, the date of the article, there were no comprehensive statistics on how many people had been victims of identity theft).

8. FTC SURVEY REPORT, *supra* note 7, at 7.

revealed an exponential increase in identity theft, with the number of victims nearly doubling each year for the previous 2-3 years.[9]

Identity theft is not a new crime. Long before the Internet, thieves used low-tech methods to obtain and misuse people's credit and identification documents.[10] Current offline identity theft techniques include simple pick-pocketing, "dumpster diving" for discarded financial records and credit card statements, stealing pre-approved credit card applications from mailboxes, completing "change of address" forms through the Post Office to divert a victim's mail, and securing low-level employment with an organization to gain access to and steal consumers' SSNs, credit reports, and financial records.[11] These techniques still account for the majority of identity theft cases,[12] but the Internet and the increased use of databases for storing consumer information has allowed thieves easier access to greater quantities of individual information at one time.[13] In close to the same

---

9. *Protecting Privacy of Social Security Numbers: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce*, 108th Cong. (2004) [hereinafter *FTC Statement 9/28/04*] (statement of Thomas B. Leary, Comm'r, FTC), *available at* http://www.ftc.gov/os/testimony/040928test.htm. The number of victims falling prey to account theft (where the thief uses a victim's existing accounts to make fraudulent purchases) has increased 71% over the last year. FTC SURVEY REPORT, *supra* note 7, at 18.

10. Brian F. Caminer, *Credit Card Fraud: The Neglected Crime*, 76 J. CRIM. L. & CRIMINOLOGY 746, 746 n.5 (1985) (noting that in 1982, "credit card fraud [was] the fastest growing crime against business" and fraud perpetrated against Visa and MasterCard amounted to $125.8 million—"two and a half times greater than the amount of money stolen in bank robberies"); *see also* Katrina Brooker, *Just One Word: Plastic; How the Rise of the Credit Card Changed Life for the FORTUNE 500—And for the Rest of Us*, FORTUNE , Feb. 23, 2004, at 125 (discussing early forms of credit card fraud).

11. Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL J.L. & PUB. POL'Y 661, 663 (1999); O'Brien, *supra* note 7; FTC, *ID Theft: What's It All About*, *at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.htm.

12. *See* FTC SURVEY REPORT, *supra* note 7, at 9.

13. *See* PETER GRABOSKY ET AL., ELECTRONIC THEFT: UNLAWFUL ACQUISITION IN CYBERSPACE 2 (2001) ("The fundamental principle of criminology is that crime follows opportunity, and opportunities for theft abound in the Digital Age."). In a 2000 Congressional Hearing, the FTC reported:

> The Internet has dramatically altered the potential occurrence and impact of identity theft. First, the Internet provides access to identifying information through both illicit and legal means. The global publication of identifying details that previously were available only to a select few increases the potential for misuse of that information. Second, the ability of the identity thief to purchase goods and services from innumerable e-merchants expands the potential harm to the victim through numerous purchases. The explosion of financial services offered on-line,

amount of time it would take for a thief to monitor a physical mailbox and steal one individual's new credit card, the thief can now set up a phishing scam and potentially steal hundreds or thousands of individuals' personal identifying information.

Once a thief has obtained a person's information, he may change the address on existing accounts and run up bills, open a new credit card account, obtain a home or car loan in the victim's name, obtain counterfeit checks to drain a person's bank account, or use a person's information when arrested for a crime.[14] Losses average $10,200 per identity theft case for businesses and $1,180 for consumers;[15] however, these costs fail to depict the full scope of the problem. In addition to monetary losses, victims report suffering non-monetary harm including emotional distress from feeling personally violated by the theft, being harassed by creditors and collection agencies for debts they did not incur, being turned down for a loan or new account, or even being arrested for crimes committed by

---

such as mortgages, credit cards, bank accounts and loans, provides a sense of anonymity to those potential thieves who would not risk committing identity theft in a face-to-face transaction.

Stana, *Identity Theft: Prevalence and Cost*, *supra* note 5, at 58; *see also* Bob Sullivan, *Database Giant Gives Access to Fake Firms*, MSNBC.COM, Feb. 14, 2004 (noting that Choicepoint, a company that maintains databases of personal information on virtually all U.S. citizens, recently warned 30,000 California residents that criminals posing as legitimate businesses had used its databases to access the residents' personal information), *at* http://www.msnbc.msn.com/id/6969799.

14. *See* FTC SURVEY REPORT, *supra* note 7, at 6 (noting that in 15% of cases, the victim's information was used for non-financial purposes, such as when the thief presented the victim's information to law enforcement when arrested for a crime or used it to obtain government documents); *see also* Saunders & Zucker, *supra* note 11, at 666-67. Saunders and Zucker present a particularly bad case discussed in *Rogan v. Los Angeles*, 668 F. Supp. 1384 (C.D. Cal. 1987), where a prison escapee who had stolen Rogan's birth certificate and used it to obtain a California driver's license also used Rogan's name when he was arrested on suspicion of murder and robbery. The identity thief was released, but the Los Angeles Police Department later issued an arrest warrant, charging Rogan with two robbery-murders. Rogan, who lived in Michigan and had no idea what was going on, was arrested at gunpoint multiple times over three years because the LAPD did not remove the warrant, even after it discovered that Rogan's fingerprints did not match those of the criminal who had used his name. Rogan won his Section 1983 civil rights action against the City of Los Angeles.

15. Jennifer Lee, *Identity Theft Victimizes Millions, Costs Billions*, N.Y. TIMES, Sept. 4, 2003, at A20. These figures are lower when the thief uses the victim's current account rather than setting up a new account in the victim's name. The FTC Identity Theft Survey also noted that many victims do not incur any out-of-pocket losses. FTC SURVEY REPORT, *supra* note 7, at 41–43. Under the Truth in Lending Act, most victims are not liable for fraudulent credit card purchases over $50, so these losses are borne by their credit issuers. *See* 15 U.S.C. § 1643(a)(1) (2000).

someone else in their name.[16] In some cases, the thief may destroy a victim's credit rating such that the victim is no longer able to obtain a loan, mortgage, or credit card. Victims average thirty or sixty hours per case trying to repair their credit history,[17] but the longer it takes victims to discover the crime, the greater the cost in terms of both financial losses and hours spent resolving the problem.[18] In the worst cases victims report spending up to 200 hours dealing with the problem, and it can take months or even years of agonizing effort for a person to clear her name and correct her credit history.[19]

Many laws criminalize identity theft and offer protection for consumers. At the federal level, laws against credit card fraud,[20] wire fraud,[21] bank fraud,[22] and identity theft[23] can be used against identity thieves. Consumers are also protected by the Truth in Lending Act,[24] which among

16. FTC SURVEY REPORT, *supra* note 7, at 47; *see also* Stana, *Identity Theft: Prevalence and Cost*, *supra* note 5, at 23 (discussing how victims feel "personally violated" by identity theft and suffer emotional harm); Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, ¶¶ 29–32 (discussing a case of criminal identity theft), *at* http://stlr.stanford.edu/STLR/Articles/04_STLR_2. Many victims also report that their problems stem from their dealings with credit reporting agencies. *See, e.g.*, Jeff Sovern, *The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules*, 64 U. PITT. L. REV. 343, 361 n.67 (2003) (discussing the extensive procedures and requirements that credit reporting agencies (CRAs) subject victims to before removing fraudulent information from their accounts, procedures to which the thieves were never subjected). Local police officers can also be less than supportive. Many do not understand their role in combating identity theft and fail to even provide victims with the police report necessary to convince CRAs to take fraudulent information off victims' accounts. *See Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions: Hearing Before Sen. Judiciary Subcomm. on Tech., Terrorism and Gov't Info.* (2000) (statement of Beth Givens, Director, Privacy Rights Clearinghouse), *available at* http://www.privacyrights.org/ar/id_theft.htm.

17. FTC SURVEY REPORT, *supra* note 7, at 6. The lower figure reflects average time spent clearing up theft that involved misuse of existing accounts, while the higher figure represents "new account" theft.

18. *Id.* at 8, 43; *see also Nowhere to Turn: Victims Speak Out on Identity Theft*, Privacy Rights Clearinghouse (May 2000) (noting that victims surveyed by the organization averaged 175 hours dealing with the theft, although seven respondents spent between 500 and 1500 hours), *at* http://www.privacyrights.org/ar/idtheft2000.htm.

19. Stana, *Identity Theft: Prevalence and Cost*, *supra* note 5, at 64-65; *see also Identity Theft and Assumption Deterrence Act of 1998*, 144 CONG. REC. S9501, 9503 (1998) (statement of Sen. Leahy).

20. 18 U.S.C. § 1029 (2000 & Supp. II 2002).

21. *Id.* § 1343.

22. 18 U.S.C. § 1344 (2000).

23. *Id.* § 1028.

24. 15 U.S.C. § 1643(a)(1) (2000).

other things limits their losses to $50 for unauthorized credit card use, and the Gramm-Leach-Bliley Act (GLB Act),[25] which prohibits a person from using false pretenses to obtain financial information from a customer. In addition, almost every state has its own criminal and consumer protection laws that deal with identity theft.[26]

There are also many stakeholders, in addition to victims and identity thieves, involved in identity theft. Federal agencies such as the FBI, Justice Department, Secret Service, and Postal Service work together and with local, state, and international law enforcement agencies to catch and prosecute identity thieves. The Social Security Administration, FTC, and state consumer protection agencies study the problem; educate consumers, law enforcement agencies, and businesses; and help consumers after their identity has been stolen. Many nonprofit organizations also help identity theft victims and work to pass tougher identity theft and consumer protection laws. The credit and financial industries, including banks, credit card issuers, and credit reporting agencies (CRAs, also called "consumer reporting agencies")[27] also play a role, as do merchants, healthcare organizations, universities, and any other organization that might be a repository for personal information.

II. PHISHING

Phishing is a particularly pernicious form of identity theft because it exacts a price on both the individual consumer and on Internet use in general. Phishing victims are subject to the same emotional and financial

25. *Id.* § 6821(b). The Gramm-Leach-Bliley Act predominantly relates to consumer privacy and financial institutions; however, the FTC has used it in civil cases against identity thieves. *See* Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Hill (S.D. Tex. 2004) (No. H 03 5537) [hereinafter FTC Complaint], *available at* http://www.ftc.gov/os/caselist/0323102/0323102zkhill.htm; Press Release, Federal Trade Commission, Justice Department Halt Identity Theft Scam (Mar. 22, 2004) [hereinafter Hill Press Release], *at* http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm.

26. *See* Holly K. Towle, *Identity Theft: Myths, Methods, and New Law*, 30 RUTGERS COMPUTER & TECH. L.J. 237, 302-305 (2004) (providing an overview of state identity theft laws, including specific code sections). This Note will discuss a few California laws as examples because California has a very high prevalence of identity theft cases relative to other states. Richard M. Stana, *Awareness and Use of Existing Data on Identity Theft* [hereinafter Stana, *Awareness and Use*], *in* IDENTITY THEFT, *supra* note 5, at 95, 104, 120. However, the sheer quantity of state laws makes a full discussion impossible in a Note of this length and breadth. In addition, some of these laws may now be preempted by the Fair and Accurate Credit Transactions Act. *See* 15 U.S.C.S. § 1681t (LEXIS Supp. 2004).

27. There are three major CRAs: TransUnion, Equifax, and Experian.

harms and damage to reputation suffered by other identity theft victims, but risk more extensive losses both financially and in time spent dealing with the problem. Merchant and credit card issuers may also suffer more extensive financial losses.[28] This is because phishing victims may not discover the theft until long after it occurs.[29]

Phishing affects the Internet in general by undermining consumers' trust in secured online transactions, which in turn leads to reduced activity online.[30] Because the fraudulent e-mails and websites look incredibly similar to official e-mails and sites, these scams call into question any electronic communication received from an online business. Consumers start to doubt the veracity of any unsolicited e-mail they receive, which could force organizations to return to more expensive offline methods to communicate with their customers.[31] In fact, research indicates that phishing and other online scams are already affecting online business. A recent survey of Internet users conducted by an e-mail security provider found that 29% of respondents stated they would avoid online shopping during Christmas 2004 due to e-mail scams.[32] A study of 39,000 Internet users in fall 2003 found that almost one-third were pessimistic about security on the Internet, in part due to online fraud—the highest figure since the company began taking the poll in 1998.[33]

---

28. The Truth in Lending Act limits consumer liability for unauthorized credit card purchases, so merchants and credit card issuers shoulder almost all of the financial losses due to fraudulent purchases. 15 U.S.C. § 1643(a)(1) (2000).

29. Because the phishing scams look so real, victims may never realize that they have been duped. Compare this to a lost or stolen wallet, where the victim knows about the theft almost immediately and can alert her credit card issuers and the CRAs before much harm has occurred. The FTC Report indicated that victims who took longer to discover that their personal information had been stolen suffered greater monetary and non-monetary losses and were at a greater risk of having new accounts opened in their name. FTC SURVEY REPORT, *supra* note 7, at 8.

30. Senator Leahy Statement, *supra* note 6; David McGuire, *Senate Bill Targets 'Phishers'*, WASH. POST., July 12, 2004, *available at* http://www.washingtonpost.com/wp-dyn/articles/A44826-2004Jul12.html.

31. *See* Brian Krebs, *Companies Forced to Fight Phishing*, WASH. POST., Nov. 19, 2004 [hereinafter Krebs, *Companies Forced to Fight Phishing*] (noting that phishing has forced businesses to change how they communicate with their customers), *available at* http://www.washingtonpost.com/wp-dyn/articles/A61916-2004Nov19.html.

32. Sullivan, *supra* note 6. *See generally supra* note 6.

33. Tedeschi, *supra* note 6 (discussing a 2003 Forrester Research poll); *see also The War on ID Theft*, RED HERRING, Oct. 29, 2004 (quoting Gartner Research analyst Avivah Litan who noted that "62 percent [of the 47 percent of adults who bank online] said they felt very nervous about security and privacy of information" and that "[e]ighty percent of that group said they'd bank and keep more money online if more security was offered by

A. Overview of Past and Present Phishing Techniques

Phishing scams involve a spoofed e-mail and a spoofed website,[34] both of which use company trademarks and logos to appear to represent a legitimate financial institution or Internet Service Provider (ISP) with which the consumer has an account. Phishing scams focus almost exclusively on banks and online shopping sites: 30% are linked to eBay or PayPal, while almost 60% target US Bank or CitiBank.[35]

Phishers use scare tactics to catch a recipient off guard. E-mails state that the recipient's account may have been compromised or will be shut down if she does not respond.[36] In the most basic phishing scams, the e-mail states that the recipient needs to update her account by clicking on a link and entering her personal and financial information in the website to which she is directed. The e-mail contains a "link alteration" that directs the recipient to a URL that looks like it should belong to the financial institution but in fact links to the phisher's website. After the recipient has entered her personal and financial information on the fraudulent website, she will then be redirected to the actual financial institution's website, to make the experience seem authentic.[37] However, by that point the victim's information has already been automatically sent to the phisher.[38] Because the whole process looks so real, a victim may not know that her identity has been stolen, and she may never trace fraudulent uses of her financial information to the phishing attack. This makes phishers particularly difficult to trace and catch.

---

service providers"), *at* http://www.redherring.com/Article.aspx?a=10938&sector=Industries&subsector=SecurityAndDefense.

34. Spoofing involves reproducing the look and feel of a website to another server owned and operated by someone else. *Spoofing Attacks*, WIKIPEDIA: THE FREE DICTIONARY, *at* http://en.wikipedia.org/wiki/Spoofing_attacks (last modified Mar. 4, 2005).

35. Krebs, *Companies Forced to Fight Phishing*, *supra* note 31; Brian Krebs, *Phishing Feeds Internet Black Markets*, WASH. POST., Nov. 18, 2004 [hereinafter Krebs, *Phishing Feeds Internet Black Markets*], *available at* http://www.washingtonpost.com/wp-dyn/articles/A59347-2004Nov18.html.

36. Saul Hansell, *Online Swindlers, Called 'Phishers,' Lure the Unwary*, N.Y. TIMES, Mar. 24, 2004, at A1 (also noting that some phishing e-mails have stated the recipient was about to be charged with child pornography).

37. Press Release, U.S. Department of Justice, Operation Web Snare 8 (Aug. 26, 2004) [hereinafter Operation Websnare Report], *formerly available at* http://www.fbi.gov/cyberinvest/websnare/websnare.pdf (on file with author).

38. *Id.* at 7.

Phishers rely almost entirely on the Internet for the ways and means of their scams. E-mail addresses are readily available online,[39] and phishers can purchase do-it-yourself phishing "starter kits" online that contain all the necessary graphics, code, text, and scripts to complete the scam.[40] Phishers then use the stolen financial information to purchase goods on the Internet.[41] Once they have stolen a victim's financial and personal information, they can sell or trade that information online as well, through news groups, chatrooms, message boards, and other covert locations.[42]

Early phishing attempts were crude and designed mainly to obtain passwords to access the Internet for free.[43] Later scams involved eBay's auction site, where thieves would use the account holder's information to set up fraudulent auctions.[44] Other early phishing attacks involving simple credit card theft were committed mainly by amateurs, including teenagers, and were relatively easy to detect.[45]

These early attacks were linked mainly to servers within the United States, but law enforcement agencies now trace the source of attacks to parts of Europe, Eastern Europe, and Asia.[46] Law enforcement agencies

---

39. *See* Operation Websnare Report, *supra* note 37, at 10 (discussing one phisher in Georgia who purchased e-mail addresses through IRC chatrooms). A Google search will turn up many websites offering e-mail addresses for sale.

40. *See* John Leyden, *DIY Phishing Kits Hit the Net*, REGISTER, Aug. 19, 2004, *at* http://www.theregister.co.uk/2004/08/19/diy_phishing.

41. Operation Websnare Report, *supra* note 37, at 10 (noting also that phishers often have these goods delivered to vacant houses or to individuals recruited for this purpose).

42. *See* Michael Cohn, *Phishing Attacks Linked to Organized Crime: Tactics Growing More Sophisticated*, SECURITY PIPELINE, July 7, 2004, *at* http://www.securitypipeline.com/22104197; Beth Cox, *The Great Credit Card Bazaar*, INTERNETNEWS.COM, Sept. 20, 2002, *at* http://www.internetnews.com/ec-news/article.php/1467331. Many of these sites have recently been shut down as part of a Secret Service operation to nab identity thieves. *See* Jim Wagner, *Feds Charge 28 in ID Theft Ring*, INTERNETNEWS.COM, Oct. 29, 2004, *at* http://www.internetnews.com/security/article.php/3429101. However, a quick Google search for the names "Carderplanet" and "ShadowCrew" revealed cached pages where users were openly selling credit card and social security numbers, both singly and in bulk, in addition to fake IDs from around the world.

43. Ramasastry, *supra* note 2; *see also* Hansell, *supra* note 36 (noting that phishing originated 10 years ago when AOL charged users by the hour. Phishers sent fraudulent e-mails to obtain AOL users' account and password information so they could access the Internet at the user's expense).

44. IFCC Intelligence Note, *supra* note 4, at 2; Krebs, *Phishing Feeds Internet Black Markets*, *supra* note 35.

45. Hansell, *supra* note 36. One set of phishing attacks was conducted by a 55-year-old woman operating out of her home in Akron, Ohio.

46. IFCC Intelligence Note, *supra* note 4, at 2; Hansell, *supra* note 36; *see also* Operation Websnare Report, *supra* note 37, at 2 (noting that "illegally obtained funds have been identified as flowing to parts of the world where [terrorist groups] have been known

also believe current attacks are linked to organized crime both inside and outside of the United States.[47] Criminals located in foreign countries are able to complete their scams with the help of individuals recruited inside the United States to receive money and merchandise.[48] These individuals re-ship the merchandise to locations outside the country and launder the money through United States and foreign bank accounts.[49]

Current attacks have become more prevalent and more sophisticated. They use spyware, take advantage of software security flaws, and are able to avoid fraud and spam filters. In one attack that uses spyware, the scam replaces the "Address" bar at the top of the victim's browser with an appropriately-designed working fake.[50] The fake address bar remains installed even after the consumer leaves the fraudulent site and allows the phisher to track the consumer's Internet movement as well as all of the information the victim sends and receives.[51] In another advanced attack, the e-mail directs the recipient to a site that appears to be under construction, but which instead takes advantage of a Microsoft Internet Explorer security flaw to install a key-logger on the victim's computer.[52] This device records a victim's keystrokes, including logins, passwords, and PINs. The key-logger also compromises the victim's computer by allowing a hacker to use it as a mail proxy for spam and by giving the hacker the ability to control the computer remotely. While Microsoft has fixed the flaw, many users do not update regularly and could still be vulnerable. In another scam, the e-mail avoids fraud and spam filters by using an image

---

to operate"). In one recent case, a thief operating out of Romania used a targeted phishing scam to bilk United States eBay purchasers out of $500,000. He was caught through a coordinated effort between the Secret Service, eBay, and the Romanian General Directorate for Combating Organized Crime. Press Release, U.S. Department of Homeland Security and U.S. Secret Service, United States Secret Service and Romanian Police Work Together to Solve Major Computer Fraud Investigation (Sept. 11, 2003), *available at* http://www.secretservice.gov/press/pub2503.pdf.

47. Cohn, *supra* note 42; Hansell, *supra* note 36.

48. Operation Websnare Report, *supra* note 37, at 8.

49. *Id.* at 9.

50. APWG Threat Advisory Alert, *Phishing Technique Replaces Web Browser Address Bar with Malicious JavaScript Fake* (Mar. 31, 2004) (noting that unlike similar attacks in 2003 that took advantage of a bug in Microsoft's Internet Explorer and thus were limited to that browser, this scam can replicate any browser), *formerly at* http://www.antiphishing.org/news/03-31-04_Alert-FakeAddressBar.html; *see also* Matthew Broersma, *Barclays Scam E-mail Exploits New IE Flaw*, ZDNET UK, Jan. 12, 2004 (discussing the flaw in Internet Explorer), *at* http://news.zdnet.co.uk/internet/security/0,39020375,39119033,00.htm.

51. APWG Threat Advisory Alert, *supra* note 50.

52. Andy McCue, *'Trojan' Emails Conceal Theft Tools*, ZDNET.COM UK, Aug. 13, 2004, *at* http://news.zdnet.co.uk/internet/security/0,39020375,39163517,00.htm.

instead of text in the body of the spoofed e-mail.[53] Other scams link to a legitimate financial institution's true site but use a "Secure Confirmation" popup screen, operated by the phisher, for the victim to enter her information.[54] In a final new attack—the worst of the recent variations—recipients are at risk even if they do not click on a link in the e-mail. If the recipient opens the e-mail, it changes her "host file," a local file on her computer that links easy-to-remember web addresses, such as www.CitiBank.com, with their IP addresses, so that whenever the consumer types in her bank's web address she is automatically directed to the phisher's IP address rather than the bank's.[55] Fortunately, this variation is not yet widespread.

These attacks are on the rise; the Anti-Phishing Working Group estimates there were over 500 unique phishing attacks per week in July 2004 alone.[56] Brightmail, an e-mail filter provider, identified 2.3 billion phishing messages in February 2004.[57] This figure represents 4% of all e-mail the company processed that month and was an increase from the 1% detected in September 2003. Although no one knows the exact cost of phishing attacks or how much money has been stolen,[58] Senator Patrick Leahy, who researched phishing to support his recent Anti-Phishing Bill, has estimated that approximately 1 million Americans have already been victims of these scams, at a cost of over $2 billion between mid-2003 and mid-2004.[59] Phishers have been able to convince up to 5% of recipients to respond to these e-mails,[60] and as the costs of running a scam are low, a 5% return rate for phishers may yield high results.[61]

---

53. Operation Websnare Report, *supra* note 37, at 8–9.

54. *Id.* at 9.

55. Bob Sullivan, *A New, More Sneaky Phishing Attack, Victim Computers Hijacked, Sent to Fake Bank Sites*, MSNBC.COM, Nov. 5, 2004, *at* http://www.msnbc.msn.com/id/6416723.

56. Anti-Phishing Working Group, http://www.antiphishing.org (last visited Feb. 3, 2005). The Anti-Phishing Working Group (APWG) is an industry association that teams software makers, banks, ISPs, and law enforcement to study and combat phishing.

57. Hansell, *supra* note 36. Brightmail was recently acquired by Symantec.

58. *Id.*

59. Senator Leahy Statement, *supra* note 6. *But cf.* Press Release, TRUSTe, U.S. Consumer Loss of Phishing Fraud to Reach $500 Million (Sept. 29, 2004) (noting that a recent report sponsored by TRUSTe estimated that "the nation's total monetary loss to victims of [phishing scams is] approximately $500 million"), *at* http://www.truste.org/about/press_release/09_29_04.php.

60. Ramasastry, *supra* note 2 (citing a study by the Anti-Phishing Working Group).

61. Most organizations, including the FBI's Internet Fraud Complaint Center (IFCC), recognize that the majority of people who receive phishing e-mails ignore or delete them, and banks think losses attributable to phishing are relatively small compared with losses due to stolen credit cards. *See* IFCC Intelligence Note, *supra* note 4; Hansell,

B. Difficulties in Deterring and Catching Phishers

Like other forms of computer crime, phishing is difficult to deter because normal barriers to offline crime do not apply.[62] Computer crime's effective anonymity means that social norms that might deter offline criminals are inapplicable to cybercriminals.[63] This anonymity also means that the chance of getting caught is significantly lower. In addition, cybercrimes such as phishing attacks are much less expensive to commit, in part because the thief's computer substitutes for the accomplices who would be needed to commit a similar crime offline.[64]

Existing federal civil and criminal laws mentioned in Part II[65] can be and have been used against phishing.[66] However, a phisher's risk of getting caught is still very low. Most consumers who enter their personal information on a fraudulent site do so because they believe the site is authentic. By the time they realize what has happened and report the scam to law enforcement, the phisher has likely disappeared without a trace. The phishers' sites are generally online for no more than 54 hours, so the spoofed site will disappear before law enforcement has even received

---

supra note 36. However, IFCC has also noted that the recent rise in identity theft and credit card fraud can be attributed, in part, to the lack of technical sophistication in new Internet users. IFCC Intelligence Note, *supra* note 4, at 1. Therefore, many are still at risk.

62. Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1011 (2001).

63. *Id.* Katyal also notes, however, that the fact that there is not more cybercrime may indicate that social norms do play some role. *Id.* at 1108.

64. *Id.* at 1042. Katyal notes that crimes committed with computers are effectively subsidized because offline criminals would need help from others and would then be criminally liable for both the underlying offense and the conspiracy, whereas criminals who work with a computer are subject only to the underlying offense. He proposes, for this reason, treating computer crime as a conspiracy, with the computer filling in as a quasi-conspirator.

65. *See supra* notes 20-25. The FTC Act, 15 U.S.C. § 45 (2000), which gives the FTC the authority to initiate federal court proceedings to protect consumers from unfair and deceptive acts, also benefits identity theft victims. Both the FTC Act and the GLB Act were used successfully in a 2004 civil case brought by the FTC against a small-scale phisher who was responsible for defrauding victims of approximately $47,000. *See* FTC Complaint, *supra* note 25; *see also* Criminal Information, United States v. Hill (E.D. Va. 2004) [hereinafter Hill Criminal Information], *available at* http://www.ftc.gov/os/caselist/0323102/0323102zkhill.htm; Plea Agreement, United States v. Hill (E.D. Va. 2004) [hereinafter Hill Plea Agreement], *available at* http://www.ftc.gov/os/caselist/0323102/0323102zkhill.htm; Hill Press Release, *supra* note 25.

66. Ramasastry, *supra* note 2.

workable information about the attack.[67] In addition, although a phisher's server information is revealed during the spoof, catching phishers is still difficult because they use multiple ISPs, redirect services, and hijacked third-party computers located in the United States and abroad.[68]

The FBI and the Secret Service have had some success catching phishers and other cyber-identity thieves. In Fall 2004, the government announced two recent investigations, "Operation Firewall" and "Operation Websnare," in which federal agencies collaborated with state and foreign law enforcement and business alliances to catch American and foreign cybercriminals.[69] Operation Websnare involved 150 investigations into crimes such as "criminal spam," identity theft, credit card fraud, intellectual property rights, and computer hacking. According to the FBI, more than 870,000 victims lost more than $210 million through these scams.[70] Operation Firewall focused on three Internet websites that provided a forum for buying and selling personal identification information and identity theft tutorials online. The Secret Service arrested 28 suspects from eight states and six foreign countries who were involved in stealing more than 1.7 million credit card numbers and other financial information costing more than $4.3 million.[71]

Although these operations involved many suspects, thousands of victims, and millions of dollars, even the FBI has stated that the investigations "represented only a fraction of the Cyber crime problem."[72] An analyst with Gartner Research, commenting on the success of Operation Firewall, noted: "It's good news when everyone works together, they can

---

67. IFCC Intelligence Note, *supra* note 4, at 2 (noting that even when victims report the attacks, they often do not include pertinent information from the e-mail, such as full header information, that would enable law enforcement to track the phisher); Ramasastry *supra* note 2.

68. Operation Websnare Report, *supra* note 37, at 7; *see also* Katyal, *supra* note 62, at 1071-74 (discussing the difficulties involved in tracing cybercriminals); Saul Hansell, *E-Mail's Backdoor Open to Spammers*, N.Y. TIMES, May 20, 2003, at A1 (discussing spammers' use of proxy servers and software to cover their tracks); Ramasastry, *supra* note 2 (discussing one scam in which the phishers moved their fraudulent website among seven different servers located all over the world over a period of just twelve days).

69. Operation Websnare Report, *supra* note 37; Wagner, *supra* note 42. The FBI is currently working with other organizations in another investigation specifically targeting phishers called "Digital Phishnet." Krebs, *Companies Forced to Fight Phishing*, *supra* note 31.

70. Operation Websnare Report, *supra* note 37, at 2.

71. Robert Lemos, *Secret Service Busts Suspected ID Fraud Ring*, CNET NEWS.COM, Oct. 28, 2004, *at* http://news.com.com/Secret+Service+busts+suspected+ID+fraud+ring/2100-7348_3-5431419.html.

72. Operation Websnare Report, *supra* note 37, at 2.

really catch the crooks. The bad news is [the criminals] are like cockroaches—you kill one and 20 pop up."[73] These investigations are unlikely to make much of a dent in the phishing problem.

III. RECENT DEVELOPMENTS IN COMBATING IDENTITY THEFT AND HOW THEY STAND UP TO PHISHING ATTACKS

This Part presents a framework for analyzing various crime control methods employed by stakeholders involved in phishing attacks. It will then use that framework to analyze recent developments in combating identity theft in general and phishing scams in particular.

A. A Framework for Phishing Crime Control

Many federal agencies, including the FTC, Justice Department, FBI, and Secret Service, are involved in efforts to protect consumers against identity theft and in prosecuting criminals who have committed theft. But the federal government cannot operate alone. Most commentators recognize that government must work with other constituents, including private business entities and potential victims, for crime control to be effective. Some even see law enforcement as having only a narrow role today because "[c]ode, market forces, and to a lesser extent social norms, have eclipsed law as the major institutions of social control in cyberspace."[74] As eBay's vice president for security noted, "Technology can solve 60 percent of the problem . . . [e]ducation and awareness can solve 20 percent, and no matter how good the industry is, there will be people who fall victims so 20 percent will have to be handled by law enforcement."[75]

Crime control, both in the physical world and in cyberspace, can be seen as occurring on three levels: primary, which includes "self-help" steps the potential victim can take to educate herself about and insulate herself from the initial crime and resulting harms; secondary, which includes architecture and fraud prevention mechanisms that private parties can institute to prevent crime and lessen the harms associated with it; and tertiary, which includes public law enforcement efforts to deter crime and

73. *The War on ID Theft*, *supra* note 33 (quoting Gartner Research analyst Avivah Litan).

74. GRABOSKY ET AL., *supra* note 13, at 8. Grabosky calls this approach "legal pluralism" and quotes Michel Foucault for the idea that crime control is a "web of constraint" in which government is but one strand. *Id.* at 6.

75. Hansell, *supra* note 36.

track down and prosecute criminals.[76] Depending on the type of crime involved and the situation, constituents at one or more of the levels may play a greater or lesser role in dealing with the crime.[77] Identity theft stakeholders who play a role at the primary level include the potential victims themselves, state and federal consumer protection agencies, and others who provide education to consumers. Insurers are also increasingly playing a role. At the secondary level are financial institutions, CRAs, and merchants. Software manufacturers and ISPs also play a role in preventing phishing attacks. Finally, the tertiary level includes local, state, and federal public law enforcement agencies. State and federal legislatures also play a role at both the secondary and tertiary levels by enacting consumer protection and criminal laws.

The past year has seen advances by constituents at each level. The rest of this Part discusses recent developments in fighting identity theft at each level, including new laws and services that help consumers secure their identity, advances in private party methods to detect and prevent fraud, and new and proposed changes to criminal laws. It also discusses the effect of these new developments on phishing attacks, analyzing which are the best methods for dealing with phishing by looking critically at which constituents are best equipped to combat this problem.

B. Primary-Level Strategies—Self-Help

We are all potential victims of identity theft, no matter how computer savvy we are and no matter how much we guard our personal information and credit card numbers.[78] This is due, in large part, to the fact that our

---

76. The following is an example of each of these levels in a car theft situation in the physical world. At the primary level, a potential car theft victim protects herself by purchasing insurance, parking in a lighted lot, and locking her car. At the secondary level, the car manufacturer protects the potential victim by installing a good locking device on the car, and the parking lot owner helps by designing the lot so that it is well lit and patrolled regularly. Finally, if both primary- and secondary-level measures fail and the victim's car is stolen, law enforcement—working at the tertiary level—properly investigates the theft, catches the thief, and uses appropriate laws to punish him for his actions and prevent him from stealing other cars in the future.

77. In the example in note 76, the potential victim can take greater responsibility for protecting herself from a car theft, whereas in a situation over which she has less control (e.g., a bank heist) she might need to be more reliant on the bank's security system (secondary level) and a quick response from law enforcement (tertiary level).

78. The greatest losses attributable to identity theft may come from corporate employees who use their insider access to steal and sell thousands of identities without the consumer ever knowing. *See* O'Brien, *supra* note 7 (discussing the "biggest case of identity theft ever" victimizing 30,000 people and perpetrated by just two individuals, one of whom worked at a software company as a help desk clerk). O'Brien also notes that the

personal information is already out in the world, beyond our control. However, there are still steps that we as potential victims can take, both to protect ourselves from theft before it happens and to insulate ourselves from its costs after it does.

Three main self-help remedies include education, insurance, and civil litigation. The first two are available to potential phishing and other identity theft victims, and the following sections will discuss them further. The third common self-help remedy—civil litigation through tort law—is less prevalent in identity theft crimes. Consumers generally do not bring lawsuits directly against identity thieves for the obvious reason that thieves are almost never caught. However, even if a thief were caught, a victim might not have recourse through civil litigation because phishing attacks probably fall under the CAN-SPAM Act, which states that the FTC is the exclusive enforcement agency and prohibits individuals from filing suit directly.[79] Consumers also do not have much recourse against organizations, such as CRAs, law enforcement, ISPs, and credit issuers, that may propagate identity theft by issuing credit or accounts to thieves under the victim's name and by refusing to remove fraudulent information from a victim's files. This gap is due in part to several laws limiting the liability of these organizations.[80] In addition, since consumers are no longer fully liable for most unauthorized purchases on their credit card, in the eyes of the law they suffer little "real" harm and often are not considered the "victim" of the fraud.[81] Although consumers suffer significant loss of time,

---

FDIC has warned that the outsourcing of corporate call centers and other high access jobs has heightened the risk of identity theft, and that even babies and the deceased have had their identities stolen. *Id.*

79. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003), Pub. L. No. 108-187, 117 Stat. 2699 (amending scattered sections of 15 U.S.C., 18 U.S.C., 28 U.S.C., and 47 U.S.C.); Michael L. Rustad, *Punitive Damages in Cyberspace: Where in the World is the Consumer?*, 7 CHAP. L. REV. 39, 73 (2004); *see also* Lily Zhang, *The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem*, 20 BERKELEY TECH. L.J. 301 (2005) (discussing the CAN-SPAM Act in more detail).

80. *See* 17 U.S.C. § 512 (2000) (limiting ISPs' liability for their customers' copyright infringement); 47 U.S.C. § 230 (2000) (limiting ISPs' liability for defamatory content published by their customers); *see also* 15 U.S.C. § 1681e(b) (2000) (requiring CRAs to maintain "reasonable procedures" to protect the accuracy of consumer records). Cases have held the standard set forth in 15 U.S.C. § 1681e(b) limits CRAs' liability. *See, e.g.*, TRW Inc. v. Andrews, 534 U.S. 19 (2001); Rustad, *supra* note 79. Rustad argues that punitive damages should be available for cybercrimes and notes that in the last 10 years "not a single consumer prevailed in a cyberlaw case in which punitive damages were awarded." Rustad, *supra* note 79, at 50.

81. *See, e.g.*, United States v. Blake, 81 F.3d 498 (4th Cir. 1996) (holding that a person whose credit card was stolen in violation of 18 U.S.C. § 1029 did not qualify as

emotional harm, and damage to reputation, the law has not been able to quantify the value of these harms and does not provide much of a remedy to identity theft victims through civil litigation.

Consumers do have other self-help remedies through education and insurance. In the last year, Congress, federal agencies, the states, and private parties have made further efforts to help consumers deal directly with identity theft by offering information and identity-theft-specific insurance policies, and by mandating and enacting procedures by which consumers may better protect their personal information before it is stolen.

1. Education

The FTC Identity Theft Survey showed that many victims of identity theft, no matter how the theft occurred, felt that the most helpful tool they could have had in dealing with the crime would have been "better awareness on their own part of how to prevent and respond to identity theft."[82] Education and awareness are especially important for phishing attacks, and may be the most effective strategies against traditional phishing[83] at any of the three levels. Unlike other forms of identity theft that occur without the victim's knowledge and in which the victim could really do nothing to protect herself,[84] identity theft through phishing is preventable if the victim knows what to look for. Phishers rely on some kind of alarming "hook," such as threat of account closure or unauthorized charges or even identity theft, to elicit an emotional reaction from recipients. But if the recipient is forewarned of this trick, she will look at the correspondence critically and not fall into the trap. Unless a recipient takes the bait and enters her personal information on the fraudulent site, the phisher cannot steal anything from her. Therefore, many losses attributable to phishing could be prevented through greater consumer awareness of the phisher's techniques.

Information on identity theft and phishing scams and how to protect oneself against them is readily available to consumers—as long as they know where to look and what to look for. Many public and private consumer groups provide this information online, and major newspapers have

---

the "victim" for purposes of restitution); *see also* Kurt M. Saunders & Zucker, *supra* note 11, at 668. Saunder and Zucker state that "no court has ever classified an individual's identity as tangible personal property." Saunder & Zucker, *supra* note 11, at 668.

82. FTC SURVEY REPORT, *supra* note 7, at 62.

83. As discussed further in this Part, education may not do much to prevent recent, more sophisticated attacks that rely less on the victim's actions and more on technology such as spyware and key-logging software.

84. *See supra* note 78 and accompanying text.

recently carried articles on identity theft.[85] The FTC has a website, hotline number, and in-depth publications that educate consumers on identity theft and phishing attacks, and how to prevent them and deal with associated problems after they happen.[86]

However, further education may not be the entire answer for many potential phishing victims. Many consumers still lack the experience to even know where to look for information on preventing identity theft and phishing, or to know what to do with the information once they learn of it. Although the FTC has tried since 1998 to be a central repository for information on identity theft and for victim complaints, its own survey in Fall 2003 revealed that only 3% of identity theft victims contacted the FTC, and only 5% contacted other federal agencies such as the Postal Service or Social Security Administration that might have directed them to the FTC website.[87] In addition, a recent survey of consumer online behavior related to identity theft suggested that even though the FTC and other organizations provided information on how to safeguard personal information online, most respondents did not follow their suggestions.[88]

Another somewhat obvious problem is that the term "phishing" is so obscure that many consumers would not associate it with a suspect e-mail purporting to be from their bank and asking for their personal information. Therefore, consumers face a Catch-22—they could prevent a successful phishing attack if they knew what to look for, but without knowing what to look for (i.e., that the scam is called "phishing"), consumers may be hard-pressed to educate themselves about the attacks.[89] This is exacerbated by the fact that the most obvious source for information—the bank or retailer that purportedly sent the fake e-mail—may not help the consumer. If the consumer tries to reach her bank via telephone, she could be in for a very long wait on hold, and if she tries to find information online, she may have a hard time locating this on the bank's website (especially if she tries to find this information by clicking on the link in the fraudulent e-mail).[90]

---

85. *See, e.g.*, O'Brien, *supra* note 7; Identity Theft Resource Center, http://www.idtheftcenter.org (last visited Mar. 7, 2005); Privacy Right Clearinghouse, http://www.privacyrights.org (last visited Feb. 3, 2005). A recent search on Google News turned up about 3,500 articles on identity theft.

86. *See* FTC, *ID Theft Home, at* http://www.consumer.gov/idtheft (last visited Mar. 7, 2005).

87. FTC SURVEY REPORT, *supra* note 7, at 50.

88. George R. Milne et al., *Consumers' Protection of Online Privacy and Identity*, 38 J. CONSUMER AFF. 217, 223-224 (2004).

89. How does one "Google" something if one does not know what it is called?

90. Banks and other financial services providers such as PayPal have improved in this area. Now many providers have links to information about phishing on their home

The banking industry has so far declined to fund a recent campaign by a privacy organization, TRUSTe, that would sponsor alternate forms of education on phishing, such as radio or television public service ads.[91]

Finally, recent phishing attacks have become more sophisticated and involve technological devices that may be beyond the ken of even relatively savvy consumers. Some of these attacks, such as those that automatically change a recipient's hostfile,[92] do not even require any action to be taken by the consumer, so she would be hard-pressed to educate herself on how best to protect herself from this type of attack. For all these reasons, even though education and awareness are important strategies in preventing phishing, other resources at each of the three levels are also required.

2. Consumer Assistance—Recent Legislative Developments

a) The Fair and Accurate Credit Transactions Act

In December 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACTA),[93] which amends the Fair Credit Reporting Act and provides measures that can help consumers correct mistakes on their credit record and protect themselves from identity theft.[94] It also mandates changes in how the credit industry takes care of a consumer's credit, although these will be discussed under secondary-level solutions below. While this new law was intended to offer more general protections against identity theft, it could also benefit phishing victims.

The FACTA was enacted to "prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, [and] make improvements in the use of, and consumer access to, credit informa-

---

pages. However, last year it was difficult to find this information, even though by then phishing attacks had become relatively common. This suggests that many institutions will still not be ready when the next version of online identity fraud hits.

91. Krebs, *Companies Forced to Fight Phishing*, *supra* note 31 (noting that TRUSTe, a nonprofit privacy group in San Francisco, has tried to convince financial institutions to fund a $10 million ad campaign to educate consumers about phishing, but as of the date of the article, none had pledged any funding).

92. *See supra* Part II.A.

93. Pub. L. No. 108-159, 117 Stat. 1952 (2003) (amending 15 U.S.C. § 1681 *et. seq.* (2000)).

94. A full analysis of this extensive piece of legislation is beyond the scope of this Note. For further information, see Gail Hillebrand, *After the FACTA: State Power to Prevent Identity Theft*, 17 LOY. CONSUMER L. REV. 53 (2004); Stefan Linnhoff & Jeff Langenderfer, *Identity Theft Legislation: The Fair and Accurate Credit Transactions Act of 2003 and the Road Not Taken*, 38 J. CONSUMER AFF. 204 (2004).

tion."[95] The Act provides that consumers have the right to request a free consumer report annually from the major CRAs.[96] It also allows consumers to put a fraud alert on their credit file if they think they have been the victim of identity theft, and establishes a national fraud alert system or a "joint fraud alert" so that once a consumer files a fraud alert with one of the three CRAs, that agency will share the request with the other two, lessening the burden on the consumer.[97] The Act also requires that CRAs block, or cease reporting, fraudulent or allegedly fraudulent information on a consumer's record when the consumer submits a police report and appropriate identifying information.[98] Some of these provisions went into effect in 2004, while others will be phased in throughout 2005.[99]

The FTC believes these new requirements will provide a large benefit to consumers by helping consumers to verify their credit information more

---

95. Pub. L. No. 108-159.

96. *Id.* § 211. Under The Fair Credit Reporting Act, the precursor to FACTA, a consumer was only entitled to a free report when he or she "suffered adverse action, believed that fraudulent information may be in his or her credit file, was unemployed, or was receiving welfare benefits." *Identity Theft: Prevention and Victim Assistance: Hearing Before the Subcomm. on Oversight and Investigations of the House Comm. on Energy and Commerce*, 107th Cong. 13 n.25 (2003) [hereinafter *FTC Statement 12/15/03*] (statement of Betsy Broder, Assistant Director, Division of Planning and Information Bureau of Consumer Protection, FTC), *available at* http://www.ftc.gov/os/2003/12/031215idtheft testimony.pdf. However, some states, including Massachusetts and New Jersey, already required that the CRAs provide consumers with free annual reports. *See* FTC, Facts for Consumers: Your Access to Free Credit Reports (Nov. 2004), *at* http://www.ftc.gov/bcp/conline/pubs/credit/freereports.htm.

97. *FTC Statement 9/28/04*, *supra* note 9. A fraud alert "is simply a statement that some information in the report may be based on identity theft." Linnhoff & Langenderfer, *supra* note 94, at 205. Linhoff and Langenderfer note that a fraud alert may prevent further damage due to identity theft because it would likely "motivate potential creditors to verify identification prior to extending credit." *Id.* at 206.

98. FACTA, Pub. L. No. 108-159 § 152. Since many police reports are automated and do not require proof of identification, the statute requires that the identity theft victim provide CRAs with additional identification, both to prevent further identity theft from fraudulently filed police reports and to prevent consumers from removing negative, but accurate, information from their reports. *See* 16 C.F.R. 603.3 (2004) (including new rules regarding proof of identity required to block fraudulent reporting); Press Release, FTC, FTC Issues Final Rules on FACTA Identity Theft Definitions, Active Duty Alert Duration, and Appropriate Proof of Identity (Oct. 29, 2004) (discussing the new rules), *at* http://www.ftc.gov/opa/2004/10/facataidtheft.htm.

99. 16 C.F.R. § 602.1; *see also Social Security Numbers and Identity Theft: Hearing Before the Subcomm. on Soc. Sec. of the House Comm. on Ways and* Means, 108th Cong. 5-6 (June 15, 2004) (statement of J. Howard Beales, III, Director, Bureau of Consumer Protection, FTC), *available at* http://www.ftc.gov/os/testimony/040615idtheftssntest.pdf.

often and learn of possible identity theft earlier.[100] FACTA will also benefit potential victims of identity theft, including people who fall for phishing attacks, by simplifying the hoops a consumer has to go through to take care of the mess in her financial records after the theft occurs.

However, FACTA's weaknesses may outweigh its benefits. FACTA continues to place the primary burden of detecting and cleaning up identity theft on the victim. It does not provide credit reports automatically and only provides them for free once a year, which may not be often enough to detect fraud.[101] This is especially problematic for phishing victims who may think that the e-mail they received from their "bank" was authentic and may not realize until much later that they have been the victim of identity theft. A phishing victim would be unlikely to seek out a credit report until she notices suspect charges on her account. If the thief has, instead, used her identity to open a new account or take out a loan in her name, she may not realize the theft has occurred until she is turned down for a loan herself. The FTC Identity Theft Survey revealed that the longer it takes for a consumer to realize that her identity has been compromised, the greater the potential damage to her credit and good name.[102] Therefore, making credit reports available for free only once a year may not provide much help for the phishing victim. If, instead, the reports were provided more often and on an automatic basis, the consumer would have a better chance of discovering the theft in time to prevent many of the worst losses.

There are other problems with FACTA. For example, while the new "joint fraud alert" system may be helpful—having a fraud alert on one's account is certainly a red flag to credit issuers—it will not necessarily prevent them from issuing credit in the victim's name to others.[103] In addition, FACTA preempts many state laws that may have offered further pro-

---

100. *FTC Statement 12/15/03*, *supra* note 96, at 13.

101. Although the annual reports are free, the law does not prevent the CRAs from trying to get consumers to purchase add-on services for a fee when they try to obtain their free report. When I obtained all three of my reports in December 2004, each agency asked me first if I would like to purchase various services ranging from my FICA score at $5.95 to an automatic identity theft detection service for $9.95 per month. Shortly after I requested my reports, I also received mail correspondence from my banks and credit card companies offering a similar monthly identity theft detection service for a fee.

102. FTC SURVEY REPORT, *supra* note 7, at 8.

103. *See* Brian Bergstein, *Anti-Identity Theft Freeze Gaining Momentum*, CNN.COM, Aug. 3, 2004 (noting that creditors may still issue instant credit despite a fraud alert); *at* http://www.cnn.com/2004/TECH/biztech/08/03/security.freeze.ap; *see also* Sovern, *supra* note 16, at 352 n.37 (noting multiple examples of this).

tection to consumers.[104] Not only would these state laws fill in the gaps in FACTA, but they would also provide an opportunity for experimentation to find the best balance between benefiting consumers and limiting the burden on the credit industry. Finally, some commentators fear that Congress may believe it has already addressed the identity theft problem and "will consider the job done and turn its attention to other matters, leaving serious gaps in the statutory matrix."[105] Therefore, while the FACTA provides some help to potential phishing victims, it is not a large change from the status quo, and it does not do much if anything to prevent identity theft before it happens.[106]

b) The "Anti-Identity Theft Freeze"

California and a few other states now offer consumers the option to put an "anti-identity theft freeze" or "security freeze" on their credit record that would prevent organizations from looking at their credit history and offering credit based on their record.[107] While the new FACTA provides identity theft victims with the ability to place a fraud alert on their credit accounts, this may not always prevent merchants and other creditors from issuing on-the-spot credit for big-item purchases.[108] The security freeze provides greater protection by completely preventing any creditor from accessing any part of a consumer's credit history—and without access, the creditor cannot offer credit. In California, this service is free for identity theft victims, although for everyone else, the initial freeze costs $10. It costs an additional $8 to lift the freeze temporarily if, for example, a consumer wants to obtain a loan or buy a car, or if she knows that someone such as a landlord will be requesting access to her account for a background check. But this cost is multiplied by three because the freeze must be performed with each of the three CRAs. The system uses a personal

104. *See* 15 U.S.C.S. § 1681t (LEXIS Supp. 2004); Hillebrand, *supra* note 94 (analyzing FACTA's preemptive effects). *But see* Robert F. Brennan, *Erroneous Federal District Court Decisions on California's Consumer Credit Reporting Agencies Act Need to be Overruled: Faith And Credit*, 27 L.A. LAW. 36 (2004) (arguing that California's identity theft laws should not be preempted by FACTA). A full analysis of FACTA's preemptive effect on state laws is outside the scope of this article.

105. Linnhoff & Langenderfer, *supra* note 94, at 215; *see also supra* note 96.

106. *See* Francis J. Menton, Jr., *Can You Protect Yourself From Identity Theft?*, N.Y.L.J., Apr. 29, 2002, at 1. Menton believes that viewing your credit report annually does nothing to prevent identity theft before it happens.

107. Bergstein, *supra* note 103. California Senate Bill 168 amended California Civil Code Section 1785.1 *et seq.*, and went into effect on January 1, 2003. *See also* LA. REV. STAT. ANN. § 9:3571.1 (West 2004); TEX. BUS. & COM. CODE § 20.034 (Vernon 2002 & Supp. 2004-2005); VT. STAT. ANN. tit. 9, § 2480h (1993 & Supp. 2004).

108. Bergstein, *supra* note 103.

identification number (PIN), and the only way to lift a freeze is by calling each of the three CRAs and providing them with the PIN.[109]

Many in the credit industry think this law is over-kill and will unnecessarily prevent easy access to credit such as quick mortgage approval—perks that consumers have come to expect.[110] In fact, only 2,000 people have taken advantage of this option in California, in part because it has not been well-publicized, and in part because it costs money and enacts a procedure that many may feel is unnecessary unless their identity has already been stolen.[111] However, victims of identity theft feel the freeze is necessary because current federal laws and practices instituted by the credit industry do not offer enough protection.[112] In addition, the law offers those who suffer damages because of a violation of the freeze to sue for injunctive relief, court costs, attorney's fees, loss of wages, and pain and suffering, when applicable, which could be beneficial, given the lack of similar remedies in the federal scheme.[113]

The freeze may be a good option for people who are more likely to be potential phishing victims. These people, who may be less savvy about identity theft or who may not want the responsibility of continually trying to educate themselves about the latest scam, could place a freeze on their records and protect themselves from inadvertent disclosure. However, for many people whose lives are more in flux—who may change jobs, residences, or accounts more frequently—the procedural hoops and financial costs required to lift a freeze could be more of an annoyance than a help.

3. Insurance

There are three main types of identify theft "insurance" now offered to consumers. Two are more like notification services than traditional insurance, and claim to deal with identity theft before it happens. The third is

---

109. Presumably, there could be some risk that a consumer's PIN would be stolen; however, as this is a unique number issued directly by the CRAs, there is less of a chance of misuse than with a commonly-used identifier such as a SSN.

110. Bergstein, *supra* note 103 (quoting a lobbyist for the Consumer Data Industry Association as calling freezes a "draconian alteration" to the credit reporting system and comparing them to "using a machine gun to get at a fly").

111. *Id.*

112. *Id.*

113. *See California Law S.B. 168 (Debra Bowen) Identity Theft Prevention*, *at* http://www.fightidentitytheft.com/legislation_california_sb168.html (last updated Sept. 14, 2004) (discussing California Law S.B. 168 and remedies provided in CAL. CIV. CODE § 1785.31 (West. Supp. 2004)). It is unclear whether these remedies are now preempted by FACTA. *See* 15 U.S.C.S. § 1681t (LEXIS Supp. 2004); Towle, *supra* note 26.

more like traditional theft insurance and covers costs incurred after a consumer's identity has been stolen.

The first type of insurance is generally offered through a consumer's bank or credit card company and may be free or may cost as much as $120 per year. The service monitors a consumer's credit activity on a daily basis and provides the consumer with regular credit reports.[114] While these services are not new, they are now being offered by more companies for less money, and consumer interest in them has grown.[115] However, many of these services do not monitor credit activity at all three CRAs, and thus could miss some fraudulent activity.[116] Furthermore, this type of insurance only protects against identity theft involving credit fraud, so it would not protect or alert a consumer against an imposter who is using her name to commit a crime. Thus, this insurance might give consumers a false sense of security that they are thoroughly insulated from identity theft.

A second type of insurance monitors the Internet for the consumer's personal identifying information and credit card numbers.[117] The service, offered by CardCops, uses a "proprietary search bot" to scan websites and chat rooms for a consumer's information, and also checks against its own list of known merchant vulnerabilities. By searching areas where identity thieves commonly buy and sell personal and financial information, the service claims to find consumer's information before it has been used for fraudulent purchases and to alert the consumer while she still has time to block her accounts.[118]

The third type of identity theft insurance operates after a consumer's information has been stolen and used fraudulently, and offers to reimburse a victim for the costs associated with restoring her good name. Coverage includes lost wages, phone bills, notary services, and sometimes attorney's fees. Some companies are now including this as part of homeowner's insurance, others are offering it as a stand-alone or add-on policy, and some

---

114. Towle, *supra* note 26. U.S. Bank offers a similar but more extensive service that not only checks consumers' credit daily with the three CRAs but also gives them access to their Social Security records and their data on file with the Medical Information Bureau, a clearinghouse that supplies medical records to insurance companies.

115. About 150,000-170,000 subscribers had signed up for Credit Watch, a service offered by Equifax, by April 2002. Sovern, *supra* note 16, at 363 n.72.

116. *See* Laura Bruce, *Is Identity Theft Protection Worth the Money?*, BANKRATE.COM, Aug. 4, 2004 (quoting Linda Foley, of the nonprofit Identity Theft Resource Center, who says, "Some check all three the first time and then monitor just one or two"), *at* http://www.bankrate.com/brm/news/advice/scams/20040804a1.asp.

117. *See generally* CardCops, *at* http://www.cardcops.com/idprotect.htm (last visited Feb. 3, 2005).

118. *Id.*

banks are offering it to all accountholders.[119] Generally these policies cost between $25 and $50 for $15,000 to $25,000 worth of coverage.[120]

These services could benefit potential phishing victims, just as they could benefit all victims of identity theft. Whether or not a consumer should purchase one of these services depends on the cost of the insurance and the person's aversion to risk. The biggest criticism of these services is not that they do not benefit the consumer, but that the banks and CRAs that offer them are capitalizing on risks they make possible, and therefore the services should be offered for free.[121] Many consumer advocates also argue that instead of providing these back-end services, banks should be instituting procedures that make these services unnecessary—such as making access to consumer files and applying for credit more difficult.[122] A final criticism is that the services do little to alert a consumer to or protect a consumer from criminal identity theft, which, although infrequent, is especially damaging to the victim. For each of these reasons, insurance alone will not solve the phishing problem.

C. Secondary-Level Strategies—Architecture and Private Party Controls

As phishing attacks become more technologically sophisticated, primary level strategies cannot be the entire answer.[123] For example, scams that covertly install spyware on a victim's computer are beyond what most consumers can be expected to understand. In addition, behavioral studies have shown that consumers are not now instituting practices recommended by the FTC to protect themselves from online fraud, possibly because they are not technically savvy.[124] Consumers will need help from private parties that have greater technological expertise and the ability to

---

119. Washington Mutual offers this service to customers with a deposit account; however, consumers must still sign up for it. There are two options. One is free and offers $5,000 in insurance to off-set recovery costs. The other costs $10 but offers $15,000 in coverage, gives consumers a copy of their credit reports, monitors consumers' credit with each of the three CRAs, and alerts consumers to any problems. Other banks offer similar products. Bruce, *supra* note 116.

120. *See Identity Theft Insurance*, Insurance Information Institute, *at* http://www.iii.org/individuals/other/insurance/identitytheft (last visited Mar. 3, 2005).

121. Sovern, *supra* note 16, at 362-363; *see id.* at 382 n.165 for further criticism of identity theft insurance; *see also* Bruce, *supra* note 116 ("[I]t should be free. It's not the consumer that has allowed identity theft to grow so explosively." (quoting Linda Foley, Internet Theft Resource Center)).

122. Bruce, *supra* note 116.

123. Ramasastry, *supra* note 2.

124. Milne et al., *supra* note 88, at 223-224 (noting that these strategies include using anonymizer software and encrypting e-mails).

make architectural changes that will prevent most of these attacks or discover them before they do too much harm.

Many commentators now believe that those who control the architecture may be in the best position to control cybercrime. Professor Lawrence Lessig has argued that architecture or "code" is better than traditional law in cyberspace because law regulates "through the threat of ex post sanction, while code, in constructing a social world, regulates immediately."[125] Relying on code rather than law may be the best way to combat other cybercrimes such as computer viruses. Even though laws criminalize the propagation of viruses, and the FBI sometimes catches these criminals, society is better protected from viruses by widespread use of virus-protection software and vigilant Information Technology (IT) professionals who discover and fix software weaknesses before they can be compromised, than by waiting for law enforcement to catch and prosecute virus propagators. This may turn out to be an effective method for preventing cyber identity theft as well.

The computer and financial industries have a vested interest in counteracting identity theft and phishing attacks. They want consumers to remain confident in doing business online,[126] and they want to protect their bottom line.[127] These organizations have the ability to make system-wide changes that could protect consumers from identity theft, and also the knowledge, financial backing and nimbleness to make these changes quickly and in direct response to real-world problems.[128]

---

125. Lawrence Lessig, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, 5 COMMLAW CONSPECTUS 181, 184 (1997); *see also* Neal Kumar Katyal, *Digital Architecture as Crime Control*, 112 YALE L.J. 2261 (2003).

126. Companies that are listed in the phishing e-mails, such as banks and merchants, are, themselves, negatively affected by these attacks. The scams use the companies' trademarks to convince the consumer the e-mail is in fact from her bank. In so doing, they are, in some senses, diluting the value of the mark, because consumers are less likely in the future to trust that the mark actually represents the product they think it does. Amazon has used this trademark argument to fight phishers. It is suing unnamed defendants under Washington state's unfair practices statute, as well as under the Lanham Act for trademark violation. *See* Amazon.com, Stop Spoofing, *at* http://www.amazon.com/exec/obidos/tg/browse/-/4060771/103-1910307-0728623 (last visited Mar. 7, 2005) (listing legal actions in which Amazon.com is a party.

127. Hansell, *supra* note 36 (quoting Earthlink's Chief Executive, Garry Betty, as saying, "We get 20,000 phone calls every time one of those [phishing e-mails] goes out, and it costs us 100 grand").

128. As an example of this capability in a different area, Katyal notes that in 2000 eBay was able to counteract denial of service attacks within 90 minutes of discovering them. Katyal, *supra* note 62, at 1092.

The Anti-Phishing Working Group has partnered with the Financial Services Technology Consortium (FSTC), an association made up of leading North American-based banks, financial institutions, research organizations and government agencies to identify and evaluate solutions to phishing.[129] The federal government, through FACTA, has instituted some changes in how the credit industry handles consumer information and is considering proposed e-mail handling changes that could affect the computer industry.[130] However, many think these groups have not done as much as they could to protect consumers.

1. Software Manufacturers and ISPs

There are two main ways to fight phishing via technology at the consumer level:[131] detect fraudulent e-mail or detect fraudulent websites. WholeSecurity, an Internet security firm in Texas, has developed software that detects fraudulent sites by analyzing web addresses and domain name registration.[132] eBay uses the WholeSecurity software, called "Web Caller-ID," in its Internet toolbar to detect fake sites purporting to be connected to either eBay or its subsidiary, PayPal. The software automatically notifies users that they are entering a fraudulent site, and it has a 98% accu-

129. Anti-Phishing Working Group, APWG and FSTC Partner on Counter-Phishing Initiative, *at* http://www.antiphishing.org/fstc-project.htm (last visited Mar. 7, 2005); Financial Services Technology Consortium, About FSTC, *at* http://www.fstc.org/about (last visited Mar. 7, 2005).

130. The FTC recently hosted an "EMail Authentication Summit" that addressed technological changes, such as domain-level authentication, that could prevent the proliferation of spam. Any development that limits spam would necessarily also reduce the amount of phishing scams, since phishers rely on spam to distribute their communications. See FTC, Email Authentication Summit, *at* http://www.ftc.gov/bcp/workshops/e-authentication/index.htm (last visited Mar. 7, 2005), for further information on the meeting and public comments on the technology from many consumer, financial, and privacy-related organizations. *See also* Zhang, *supra* note 79.

131. This Note will not discuss back-end technological developments used by credit organizations to protect personal information in their databases, nor will it discuss technological developments used by these organizations to detect fraud. Merchants and banks use software that looks for "red flags" to alert the vendor to possible credit card fraud. For example, BestBuy has software that can be programmed to automatically reject any online orders that originate from countries with high fraud rates. Brian Hansen, *Cyber-Crime*, CQ RESEARCHER, Apr. 12, 2002, at 311. The FTC, through FACTA, will be working with the financial industry to develop these indicators. *FTC Statement 9/28/04*, *supra* note 9, at 3. This kind of fraud detection brings its own privacy concerns—the only way a bank can tell whether a person trying to impersonate you is really not you is if the bank knows a lot about you and your habits.

132. Alorie Gilbert, *Catching 'Phishers' a WholeSecurity Sport*, CNET NEWS.COM, Aug. 16, 2004, *at* http://news.zdnet.com/2100-1009-5312105.html.

racy rate.[133] Earthlink also offers a downloadable toolbar that alerts a user before she visits a fraudulent site by comparing the URL against the toolbar's list of known fraudulent sites and by analyzing unknown sites for fraudulent tactics.[134] This service seems to have been successful; Earthlink has been able to reduce its costs in customer support calls, even though it remains among the top-ten companies most targeted by phishing attacks.[135]

Other companies have developed software that detects fraudulent e-mails. Microsoft has developed e-mail authentication technology called "SenderID" to combat "spoofed" return addresses on e-mails.[136] SenderID validates the sender's server IP address to "assure an e-mail recipient that a message claiming to be from a credit card company actually is."[137] However, like many Microsoft products, this technology has come under fire recently. The Apache Foundation, an open-source development group, claims that Microsoft's licensing requirement is too strict. The group thinks the license is "incompatible with open source [and] contrary to the practice of open Internet standards."[138] In part due to the rejection of SenderID by the open-source community, AOL has decided not to use the product.[139]

These technologies have additional drawbacks. Microsoft's SenderID raises privacy concerns because it would require mail service providers to tell Microsoft about customers using SenderID.[140] In addition, consumer organizations such as the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center fear that e-mails that identify the sender could lead to even greater data collection by private marketers and

---

133. *Id.*

134. Earthlink, *at* http://www.earthlink.net/home/software/toolbar (last visited Mar. 7, 2005).

135. Krebs, *Companies Forced to Fight Phishing*, *supra* note 31. EarthLink now receives about 300 phone calls and spends just under $5,000 per incident, a big reduction from an earlier per-incident figure of 20,000 calls at $100,000. *Id.*; *see also* Hansell, *supra* note 127.

136. Dawn Kawamoto, *Microsoft Touts 'Sender ID' to Fight Spam, Scams*, CNET NEWS.COM, Aug. 12, 2004, *at* http://news.com.com/Microsoft+touts+%27Sender+ID%27+to+fight+spam%2C+scams/2100-1029_3-5307339.html.

137. *Id.*

138. Robert Lemos, *Apache, Open-Source Groups Wary of Sender ID*, CNET NEWS.COM, Sept. 2, 2004, *at* http://news.com.com/2100-1013_3-5345317.html.

139. David F. Gallagher, *Users Find Too Many Phish in the Internet Sea*, N.Y. TIMES, Sept. 20, 2004, at C4.

140. Lemos, *supra* note 138.

surveillance by law enforcement.[141] Sender identification also impacts free expression and anonymity, core principles in the United States.[142] Software that targets fraudulent sites could also be problematic if it is not subtle enough to discern the difference between a scam and a parody.

These issues should be balanced against a decision to institute technological changes, especially if the benefits of the changes are minor compared to the threats to privacy and free expression. If the technology allows consumers to have some control over which sites they see or e-mails they receive (like spam filters do), then it could be a welcome addition to the potential phishing victim's arsenal. However, if it forces a consumer to choose between relinquishing privacy in her e-mail or online actions and being subjected to further phishing scams, which she could combat using less intrusive strategies, she should choose the latter.

2. *The Credit Industry: Credit Card Issuers, Merchants, and CRAs*

Laws at the state and federal level require credit organizations to institute practices that protect consumers' identifying information[143] and also limit consumer liability for fraudulent charges.[144] This Section discusses a few recent legal developments that affect the credit industry and that could benefit potential phishing victims.

Banks, merchants, and credit card vendors are the most common organizations contacted by consumers after they have been victims of identity theft.[145] FACTA, in addition to providing consumers with new tools to

---

141. *See, e.g.*, EFF Comment to FTC Summit, *at* http://www.ftc.gov/os/comments/emailauthentication/512447-0043.pdf (last visited Mar. 7, 2005); Electronic Privacy Information Center, *Privacy*, *at* http://epic.org/privacy (last modified Jan. 11, 2005). EFF distinguishes between e-mail authentication and e-mail identification; it supports the former but does not support the latter.

142. *See generally* Peter J. Dugan, *National Security Checks Are in the Mail: A First Amendment Analysis of Intelligent Mail and Sender Identification*, 12 COMMLAW CONSPECTUS 265 (2004).

143. *See* Fair Credit Reporting Act, 15 U.S.C. § 1681 *et. seq.* (Supp. II 2002); *see also* Towle, *supra* note 26, at 308-310 (discussing some of these state laws).

144. 15 U.S.C. § 1643(a)(1) (2000) (limiting consumer liability for fraudulent credit card purchases to $50); *see also id.* § 1693 (providing consumer protection for all transactions using a debit card or electronic means to debit or credit an account). For interesting discussions of the history of credit cards and laws that affect them, see David G. Adams & Marlene Feigin Schwartz, *Consumer Protection*, 1976 ANN. SURV. AM. L. 257, 302 (criticizing the law for not affecting the majority of credit card transactions because the typical purchase in the 1970s was less than $50); Brooker, *supra* note 10.

145. FTC SURVEY REPORT, *supra* note 7, at 50 (noting that 43% of identity theft victims contacted these organizations while 22% contacted CRAs).

help themselves fight identity theft, mandates several changes in how credit bureaus and merchants handle consumers' credit. It requires CRAs to institute account blocking when a consumer submits a police report of identity theft, requires businesses to truncate credit card numbers on receipts, and mandates that FTC and banking regulators work together to develop red-flag indicators of ID theft.[146]

State laws provide further protections. For example, California law requires companies that maintain an unencrypted database of personal information to notify their customers if their information has been acquired by an unauthorized person.[147] California also requires organizations to limit their dissemination of SSNs[148] and requires lenders who discover that the personal information offered in a credit application does not match the information on a consumer's credit report to take reasonable steps to verify the information, including informing the consumer.[149] Consumers who are damaged by a violation of these statutes may recover actual damages, attorney's fees, and punitive damages up to $30,000.[150] However, FACTA has extensive and specific preemption provisions,[151] so it is unclear where these state laws now stand.

---

146. *FTC Statement 12/15/03*, *supra* note 96, at 13-14; *see also supra* note 131. Banks already develop these indicators on their own. *See* Sovern, *supra* note 16, at 372 n.116.

147. CAL CIV. CODE §§ 1798.29, 1798.82-.84 (West Supp. 2004); *Identity Theft: Hearing Before the House Subcomm. on Tech., Info. Policy, Intergov't Relations, and Census of the Comm. on Gov't Reform*, 108th Cong. 13 n.9 (2004) (statement of Orson Swindle, Commissioner, FTC), *available at* http://www.ftc.gov/os/2004/09/040922infosecidthefttest.pdf; Jaikumar Vijayan, *One Year Later, California Identity Theft Law Remains Low-Key*, COMPUTERWORLD, June 7, 2004 (discussing the effectiveness of the new law), *at* http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,93667,00.html; *see also* Sullivan, *supra* note 13 (noting that when Choicepoint's databases were breached it complied with this law and alerted 30,000 California residents whose information had been accessed fraudulently; although Choicepoint has information on almost every U.S. citizen, no other state's residents were contacted).

148. CAL. CIV. CODE § 1798.85. This law prevents a "person or entity" from publicly posting or displaying an individual's SSN, printing it on a card, or requiring it to be transmitted over an unsecure Internet connection. It also restricts organizations from printing SSNs on some information mailed to individuals. *Id.*

149. *Id.* § 1785.20.3(a); Dan Verton, *Regulatory Requirements Place New Burdens on IT: Calif. Privacy Law to Debut; Panic Emerging*, COMPUTERWORLD, June 30, 2003, *at* http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,82600,00.html.

150. CAL. CIV. CODE § 1785.20.3(c).

151. *See* 15 U.S.C.S. § 1681t (LEXIS Supp. 2004).

Many commentators and victims of identity theft do not believe these laws meaningfully protect personal information from identity theft.[152] For example, despite lobbying efforts by consumer groups, FACTA does not include any provisions that address the widespread overuse of SSNs as identifiers, which many see as the biggest reason for the current identity theft problem.[153] Often credit issuers will issue credit based almost completely on a SSN. If the thief has this number correct, he can still receive credit despite misspelling the victim's name and using a different address.[154]

Without strict regulation, the credit industry is doing little on its own to prevent identity theft. Banks, credit card companies, and other vendors noticed "suspicious account activity" in only 25% of cases reported in the FTC Survey.[155] Moreover, CRAs, which generally are not liable for reporting inaccurate information and bear no financial liability for fraudulent purchases,[156] do not search for or disclose potential fraud to consumers unless the consumer requests her credit report or pays for a notification service. Most consumers do not discover that their identifying information has been compromised until *they* take steps to access their credit, such as monitoring their own account activity or attempting to obtain credit, at which point it may be too late to prevent much of the damage.[157]

Many think this is a poor record for companies that have most of the control over access to consumers' information.[158] Banks, merchants, and credit card vendors admit that they are in the best position to develop efficient fraud prevention measures,[159] yet many financial services firms that collect personal information online do not use security features to protect that information.[160] Banks also contribute directly to the phishing problem

152. *See generally* Linnhoff & Langenderfer, *supra* note 94; Sovern, *supra* note 16.

153. Linnhoff & Langenderfer, *supra* note 94, at 215; Valetk, *supra* note 16, ¶ 21.

154. Valetk, *supra* note 16, ¶ 22.

155. FTC SURVEY REPORT, *supra* note 7, at 39.

156. 15 U.S.C.S. § 1681e(b) (LEXIS Supp. 2004) (requiring CRAs to maintain "reasonable procedures" to protect the accuracy of consumer records). Sovern argues this accuracy standard is inadequate to protect consumer information, and the cases he cites support his point. Sovern, *supra* note 16, at 390-93 & n.191.

157. FTC SURVEY REPORT, *supra* note 7, at 39-40.

158. *See also* O'Brien, *supra* note 7 (discussing a Gartner Research survey criticizing the financial industry for "not putting into effect more rigorous computer screening procedures to protect customer accounts" which has, in turn, "forced identity theft victims to bear most of the crime's social and economic costs"). *See generally* Sovern, *supra* note 16.

159. Sovern, *supra* note 16, at 374 n.119.

160. Jane Black, *Basic Hygiene for Sensitive Data*, BUSINESS WK. ONLINE, Nov. 14, 2003, *at* http://www.businessweek.com/technology/content/nov2003.

by sending out e-mail messages that look similar to phishing scams: offering deals on balance transfers and requiring customers to click on a link in the e-mail to access the deal.[161]

Banks argue that they are doing what they can and have a financial incentive to prevent identity theft—under the Truth in Lending Act, they are liable for fraudulent credit card purchases over $50.[162] The losses associated with identity theft support their argument. The FTC Identity Theft Survey revealed that last year identity theft cost businesses $47.6 billion.[163] However, MasterCard and Visa estimated that annual total fraud losses due to identity theft represented only 1/10th of one percent of annual sales volume, which belies the argument that credit issuers have a financial incentive to prevent identity theft.[164] Credit-issuing organizations also pass these losses on to their customers through higher interest rates and late charges, so any small losses they incur are fully paid for by the consumer.[165] CRAs seem to have only a negligible incentive to prevent identity theft, because they are not financially liable for fraudulent purchases and are also generally not liable for reporting inaccurate information. A final mark against the credit industry is the simple fact that the incidence of and costs associated with identity theft continue to increase almost exponentially year by year, despite the industry's purported efforts to prevent it. A law review article in 1985 noted that, around that time, credit card fraud was the "fastest growing crime against business,"[166] yet this is still the case more than twenty years later. Since these organizations admit they could prevent fraud, they are clearly not doing as much as they could.[167]

---

161. Krebs, *Companies Forced to Fight Phishing*, *supra* note 31.

162. 15 U.S.C. § 1643(a)(1) (2000).

163. FTC SURVEY REPORT, *supra* note 7, at 7.

164. Stana, *Identity Theft: Prevalence and Cost*, *supra* note 5, at 22, 50. These losses are incurred by banks that issue credit under the MasterCard or Visa name. Visa and MasterCard do not offer credit themselves and therefore do not suffer these losses.

165. Sovern, *supra* note 16, at 368 nn.86-87.

166. *See* Caminer, *supra* note 10, at 746.

167. Victims of identity theft were also unimpressed with the consumer service they received when they contacted these organizations. One identity theft victim said, "My anger at my perpetrator quickly transferred to the credit-granting community itself... They don't care what this does to victims because they don't have to care." O'Brien, *supra* note 7. Thirty-one percent of identity theft victims who contacted multiple CRAs were "dissatisfied" with all of the CRAs they contacted. FTC SURVEY REPORT, *supra* note 7, at 55. Satisfaction was higher for those who contacted credit card companies: only 10% were dissatisfied when the consumer had one card misused, and 18% were dissatisfied when they had more than one card misused. *Id.*; *see also* Sovern, *supra*

Victims surveyed in the FTC study noted ways in which they thought the financial services industry could improve both its procedures for handling consumers' information and for dealing with consumers after their identity has been stolen. These suggestions included implementing improved authentication measures during transactions, making greater efforts to monitor consumers' account activity, and notifying consumers when unusual transactions occurred.[168] Victims also thought institutions could improve their follow-up and assistance by "listening to the victim and treating them with more understanding and less suspicion."[169]

Professor Jeff Sovern has argued that if the credit industry were held liable to consumers for identity theft-related damages when it could have prevented the theft, this would induce the industry to find the best ways to protect consumer information.[170] He argues this incentive would be better than changing or strengthening regulatory laws because instead of mandating procedures that may not be cost-effective and may be outdated quickly, it would allow the credit industry to be flexible in its responses to identity theft and to find its own best solutions.

The credit industry could make many changes that would benefit identity theft victims and that would in turn benefit potential phishing victims. However, without further financial incentives or stronger regulatory laws, it seems unlikely the industry will institute these changes on its own. Therefore, potential phishing victims cannot rely solely on the credit industry to protect them from identity theft.

D. Tertiary-Level Strategies—Public Law Enforcement

Law enforcement generally only plays a role in crime control when measures at the other two levels have failed. This is in large part because law enforcement does not have the resources to attend to all crimes. This is especially true when it comes to sophisticated and coordinated identity theft scams such as phishing, which are difficult and costly to investigate and prosecute.

---

note 16, at 367 n.64, 368 n.66 (recounting stories and statistics on CRAs' poor customer service record).

168. FTC SURVEY REPORT, *supra* note 7, at 63.

169. *Id.*

170. *See generally* Sovern, *supra* note 16. Sovern argues that changing loss allocation rules so that the credit industry bears more of the costs of identity theft and the consumer bears less would spur the credit industry to make better changes than those the federal government has instituted. *Id.*

The main federal criminal laws used against identity thieves include the Credit Card (or "Access Device") Fraud Act[171] and the Identity Theft and Assumption Deterrence Act of 1998 (ID Theft Act).[172] The Credit Card Fraud Act makes it a felony to "knowingly and with intent to defraud," use, purchase goods aggregating $1,000 or more with, or possess fifteen or more unauthorized "access devices."[173] Access devices include account numbers and personal identifiers that can be used to "to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds."[174] The Credit Card Fraud Act includes penalties of up to 15 years and a fine.[175] It also allows for restitution to the "victim," although the Act considers the bank, credit issuer, or merchant to be the victim rather than the person whose identity was stolen, because the credit issuer is financially liable for the fraudulent purchases.[176]

The ID Theft Act includes similar penalties for the unauthorized transfer or use of "means of identification."[177] The ID Theft Act does not ex-

---

171. 18 U.S.C. § 1029 (2000 & Supp. II 2002). This statute was called the "Credit Card Fraud Act" when it was first passed in 1984. Although it now covers fraud that extends beyond credit card misuse, I will continue to call it by its 1984 name as a shorthand.

172. Pub. L. No. 105-318, 112 Stat. 3007 (1998) (amending 18 U.S.C. § 1028). Almost all states have also enacted laws criminalizing identity theft. *See* Stana, *Identity Theft: Prevalence and Cost*, *supra* note 5, at 25 n.13.

173. 18 U.S.C. § 1029. Courts have also construed mere possession of counterfeit access devices to be a violation of the Act. *See, e.g.*, United States v. Scott, 250 F.3d 550 (7th Cir. 2001).

174. 18 U.S.C. § 1029(e)(1) (2000) states that:

> the term 'access device' means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

Courts have also held that a person can be charged with separate offenses for each unauthorized use of a credit card in excess of $1,000 (rather than aggregating the uses into one count). *See e.g.*, United States v. Iredia, 866 F.2d 114, 120 (5th Cir. 1989).

175. 18 U.S.C. § 1029(c)(1)(A)(ii) (Supp. II 2002).

176. *See supra* note 81; *see also Identity Theft: Hearing Before the Fin. Insts. and Consumer Credit Subcomm. of the House Financial Services Comm.*, 107th Cong. n.4 (2003) (statement of J. Howard Beales, III, Director, Bureau of Consumer Protection, FTC), *available at* http://www.ftc.gov/os/2003/06/030624idthefttestimony.htm.

177. 18 U.S.C. § 1028(a)(7) (2000). "Means of identification" include a person's name, date of birth, social security number, driver's license number, passport number, "electronic identification number, address or routing code," and "unique biometric data,

plicitly govern theft of credit card or bank numbers, which are considered "access devices" and protected under the Credit Card Fraud Act.[178] However, the United States Sentencing Commission has recognized that the unauthorized use of credit cards may be prosecuted under either or both of these statutes.[179] In fact, the Sentencing Commission has recognized that the ID Theft Act covers criminal activities that could also be independently prosecuted via about 180 other federal criminal statutes.[180]

The biggest difference between the Credit Card Fraud Act and the ID Theft Act is that the ID Theft Act considers the "victim" to be the person whose identity was stolen, and allows sentencing enhancements based on factors such as the number of victims and the harm done to their reputation.[181] It also enables law enforcement to initiate an investigation earlier because it criminalizes the act of stealing the information with intent to perpetrate a fraud rather than the use of that information for fraudulent purposes.[182] However, it too does not include a restitution provision for a person whose identity has been stolen, so the fact that it characterizes this person as the victim is not much of a benefit.[183]

Various problems with law enforcement specific to phishing and other sophisticated forms of identity theft make the use of federal and state laws difficult. For example, jurisdictional issues can prevent proper investigation at the state or local level.[184] Victims' first line of defense is their local police department, but while victims may be able to file a police report in their own state,[185] they may not be able to do so in the location where their

---

such as fingerprint, voice print, retina or iris image." 18 U.S.C.S. § 1028(d)(7)(A)-(C) (LEXIS Supp. 2004).

178. 18 U.S.C. § 1029(e)(1) (2000).

179. *See* Stana, *Awareness and Use*, *supra* note 26, at 97.

180. *Id.* at 98.

181. Kristen S. Provenza, *Identity Theft: Prevention and Liability*, 3 N.C. BANKING INST. 319, 325 (1999).

182. *Id.* at 324.

183. *See* Saunders & Zucker, *supra* note 11, at 671. The Senate version of the bill included a restitution provision, but this version did not pass. Thus, "federal courts are precluded from awarding restitution to individuals who incur expenses associated with the theft of their identities." *Id.*

184. Katyal, *supra* note 62, at 1018–19 (noting that the patchwork of state laws addressing cybercrime are ineffective due to the difficulty in tracking cybercrime and enforcing laws across jurisdictions).

185. Victims may not be able to file a police report at all—the FTC Report and many other consumer organizations have noted that local police often do not fully understand the criminal nature of identity theft and recommend that victims talk with their credit card company rather than file a report. This can be problematic because many of the new information-blocking services are only available to consumers who can provide a police

information was actually used fraudulently.[186] Another problem is that local police may not want to spend limited resources investigating a crime that has occurred in another jurisdiction and can be passed off to that jurisdiction. Finally, phishing attacks and other online scams present a challenge to law enforcement because they are designed to appear to be disconnected and small-scale, when in fact they are coordinated and large-scale.[187] The FTC is trying to combat all of these problems through a program called the "Consumer Sentinel Network," which is accessible to law enforcement agencies across the country and links to an "Identity Theft Data Clearinghouse" containing over 666,000 consumer complaints.[188] However, out of an estimated 18,000 state and local law enforcement agencies in the United States, only about 1,040 agencies have signed up for access to the network so far.[189] Thus, both the FTC and local law enforcement have a long way to go to provide more of a benefit to the phishing victim.

Jurisdictional issues also affect federal law enforcement efforts because phishing scams are increasingly operating across national borders. The physical evidence and contraband may be located anywhere on the planet, and phishers may be operating out of countries that do not have laws criminalizing their conduct, thus preventing extradition due to the dual criminality doctrine.[190] In addition, United States evidence and crimi-

---

report. *See supra* note 16; *see also* O'Brien, *supra* note 7 (discussing victims' problems with trying to file a police report).

186. Stana, *Identity Theft: Prevalence and Cost*, *supra* note 5, at 24.

187. Krebs, *Companies Forced to Fight Phishing*, *supra* note 31.

188. *FTC Statement 9/28/04*, *supra* note 9; *see also Consumer Sentinel*, *at* http://www.ftc.gov/sentinel (last visited Mar. 7, 2005).

189. *FTC Statement 9/28/04*, *supra* note 9 (noting that as of September 2004, "more than 1042 law enforcement agencies" had signed up for access to the database); Stana, *Awareness and Use*, *supra* note 26, at 119 (noting that there are approximately 18,000 state and local law enforcement agencies in the United States). For example, as of 2002, the Los Angeles Police Department, one of the largest investigators of identity theft in the country, did not subscribe to the Network. Over 8,000 cases of identity theft were reported to the LAPD during calendar year 2001, and relative to other states, California has a very high prevalence of identity theft cases. Stana, *Awareness and Use*, *supra* note 26, at 104, 120.

190. Katyal, *supra* note 62, at 1095 n.244. The dual criminality doctrine provides that if two countries have overlapping criminal laws, a criminal located in one country may be extradited to or prosecuted in the other country, even if the two countries' specific criminal laws are not included in the treaty between them. *See* Amalie Weber, Note, *The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 425, 426–428 (2003) (discussing the doctrine and other jurisdictional issues facing international cybercrime investigations). *See generally* Marian Nash (Leich), *Contemporary Practice of the*

nal procedure laws may prevent some criminals arrested in foreign countries from going to trial in the United States—for example, if foreign search and seizure or taking-of-testimony practices are inconsistent with United States standards.[191]

Federal law enforcement and investigation agencies also may not help the individual victim because they operate at a higher level than individual crimes. The Secret Service has shifted its focus from investigating "'street crime' level offenders" to individuals and groups involved in systematic, high-dollar crimes with a broader community impact.[192] The FBI has also moved in this direction: it tries to bundle smaller cases into larger "high-profile, high-impact prosecutions" before it tries to get resources to prosecute them.[193] The FBI also does not get involved until victims' losses total more than $50,000,[194] a figure that is much higher than losses that most if not all individual phishing victims and other victims of identity theft will ever suffer.

Most victims of identity theft must have a sense of these problems with law enforcement because most never report their case to law enforcement.[195] Of those who report, almost a third were "very dissatisfied" with the response they received.[196] Victims felt law enforcement could improve the investigation of identity theft through a stronger commitment to catching the thief, better follow-up and communication, and increased assistance.[197] Many also thought penalties for thieves should be stiffer.

Unfortunately, recent developments in the law have not addressed many of these core concerns. Instead of increasing resources and training for law enforcement, legislators have chosen to focus on stiffer penalties and trying to pass more specialized laws.[198] During the summer of 2004, in response to the increasing frequency of identity theft scams such as

---

United States Relating to International Law, 92 AM. J. INT'L. L. 44 (1998) (discussing the use of "dual criminality" clauses in treaties).

191. *See* GRABOSKY ET AL., *supra* note 13, at 10.

192. Stana, *Identity Theft: Prevalence and Cost*, *supra* note 5, at 43.

193. O'Brien, *supra* note 7; *see supra* Part II.B (discussing Operations Websnare and Firewall).

194. Krebs, *Companies Forced to Fight Phishing*, *supra* note 31.

195. FTC SURVEY REPORT, *supra* note 7, at 9.

196. *Id.* at 61.

197. *Id.* at 62.

198. Katyal notes that the standard solution to the problem of lack of cost deterrence in cybercrime is to increase the penalties. Katyal, *supra* note 62, at 1011. However, it is difficult to increase the penalties enough to compensate for the low probability of catching thieves without creating a completely disproportionate and cruel sentence. *See id.* at 1040.

phishing, the vast costs attributable to identity theft, and terrorist attacks, Congress passed a new law called the Identity Theft Penalty Enhancement Act (ITPEA).[199] This Act does not change the substantive identity theft laws but does increase penalties for identity theft-related crimes. It also creates a new crime of "aggravated identity theft," defined as using a stolen identity to commit other crimes.[200] The law adds a minimum sentence of two years to any felony punishment for crimes committed using the stolen personal information[201] and a five-year sentence enhancement if the stolen identity was used during a terrorism offense.[202]

This new change in the law would only affect phishing if the phisher were caught and prosecuted under the ID Theft Act. This raises two issues. First, since phishers are so hard to catch, adding on two to five years to a sentence probably will not act as a deterrent for a crime that already may have a 15 year sentence.[203] Moreover, like most criminals, phishers do not think they are going to get caught.[204] Thus, "tougher sentencing laws would only induce 'false guilty pleas' by innocent defendants who do not want to risk trial."[205] This likelihood is buttressed by the Justice Department's statements that sophisticated criminals are much better at covering their tracks (for example, through use of anonymizer software), while less-sophisticated criminals leave "fingerprints," making them easier to catch.[206] This suggests law enforcement will not be able to catch the worst criminals, and the longer sentences under the ITPEA may become disproportionate to the crime of those who are actually caught.

The second reason why this change will have little affect on phishing attacks is because other laws, such as the Credit Card Fraud Act may be more appropriately used against these criminals. In one recent case against a phisher, the Justice Department chose to prosecute him under the Credit Card Fraud Act rather than the ID Theft Act, despite the fact that his theft of social security numbers and other identifying information would subject

199. Pub. L. No. 108-275, 118 Stat. 831 (2004) (to be codified at 18 U.S.C. § 1028A); *see* Ramasastry, *supra* note 2.

200. Pub. L. No. 108-275, § 2, 118 Stat. 831; Ramasastry, *supra* note 2.

201. Pub. L. No. 108-275, § 2, 118 Stat. 831.

202. *Id.*

203. Declan McCullagh, *Season Over for 'Phishing'?*, CNET NEWS.COM, July 15, 2004, *at* http://zdnet.com.com/2100-1105_2-5270077.html.

204. Hansen, *supra* note 131, at 322.

205. *Id.*

206. *See* Katyal, *supra* note 62, at 1073 n.185 (citing James K. Robinson, Remarks at the International Computer Crime Conference: Internet as the Scene of Crime (May 29-31, 2000)), *at* http://www.usdoj.gov/criminal/cybercrime/roboslo.htm).

him to liability under that act as well.[207] As crimes covered by the ID Theft Act could also be prosecuted via 180 other federal criminal statutes,[208] it is unclear whether this law will ever be used.

Another problem in efforts to combat phishing scams and to prevent consumers from suffering loss stems from limitations within the laws. Most laws that could be used against phishers require proof that a victim suffered "measurable losses,"[209] so the laws cannot take effect until after a consumer has already been defrauded.[210] Since most phishing sites remain online for only a short amount of time,[211] by the time a consumer realizes she has suffered "measurable losses" and has filed a complaint with law enforcement (if one is ever filed) it may be too late to catch the thief.

In response to this problem, Senator Patrick Leahy introduced a bill in July 2004 that would have criminalized phishing before a person is defrauded.[212] While this bill did not pass out of committee, it is useful to discuss it as a possible solution against phishing because its purpose was more to protect consumer confidence in the Internet, rather than individual phishing victims. The proposed bill would have made it illegal to create a website that misrepresented itself as a legitimate online business in order to induce a person to transmit personal identification.[213] It would also have made it illegal to knowingly send out spoofed e-mails that linked to these websites with the intention of committing a crime of fraud or identity theft.[214] The penalty for each new crime would have been a fine and/or up to five years imprisonment.[215] Senator Leahy argued that it was important to target scams before they have defrauded anyone of any money to prevent "one of the greatest harms caused by phishing: a diminished trust in the Internet's system of addressing and linking" and to protect the "integrity" of the Internet itself.[216]

Professor Kaytal echoes the importance of such protections. He suggests that crimes that "undermine interconnectivity should be singled out for special disfavor,"[217] and compares these scams to offline crimes such

207. *See* Hill Criminal Complaint, *supra* note 65; Hill Plea Agreement, *supra* note 65; Hill Press Release, *supra* note 25.
208. Stana, *Awareness and Use*, *supra* note 26, at 98.
209. McGuire, *supra* note 30.
210. Ramasastry, *supra* note 2.
211. *Id.*
212. Anti-Phishing Act of 2004, S. 2636, 108th Cong. § 1351 (2004).
213. *Id.* §1351(a).
214. *Id.* §1351(b).
215. *Id.* §1351.
216. Senator Leahy Statement, *supra* note 6.
217. Katyal, *supra* note 62, at 1088.

as bombing a major highway or a club where people go to interact. Kaytal argues that "[w]e punish not simply because of the harm to the individual victim, but because the crime fragments trust in the community, thereby reducing social cohesion and creating atomization."[218] While these are valid arguments, they may not demonstrate a true need for such a specific and limited law as Senator Leahy's proposed bill. Operations Websnare and Firewall demonstrate that law enforcement already has laws it can use against phishers. The real problem seems to be lack of resources and incentive rather than lack of laws. Considering the difficulties involved in tracking and catching phishers, a new, more specialized law probably would not make much of a difference.

Even if Senator Leahy's bill had passed, it would not have reached all phishers. As noted above, most victims of identity theft do not report the crime to law enforcement. In addition, many phishers operate overseas; even if United States jurisdiction under this proposed law could reach to foreign countries, the United States might not be able to extradite criminals due to dual criminality problems. There also may be some question about whether we want to criminalize an act before anyone is really harmed, and whether this new law adequately addresses parody and First Amendment concerns.[219] Senator Leahy's bill stated that it protected against criminalizing a legitimate parody website or e-mail by requiring that the actor have the *intent* of committing a crime of fraud or identity theft. However, this might place too much discretion in the hands of law enforcement. For all these reasons, Senator Leahy's anti-phishing bill might have been helpful, but would not have solved the phishing problem.

IV. CONCLUSION

Phishing differs from many other types of identity theft in that it relies on an active response from the victim. In most attacks, if the victim does not fall for the scam and does not enter her personal information, the thief cannot steal anything from her. As such, it is both simpler and more difficult to combat—simpler because an educated and aware recipient should not be fooled, but more difficult because an uneducated recipient may fall for the bait, enter her personal information, never realize that that was how her identity was stolen, and thus thwart any chance for law enforcement to track and catch the thief. This conundrum necessitates coordinated efforts between potential victims, law enforcement agencies, and other organiza-

218. *Id.* at 1089.

219. *See, e.g.*, IFCC Intelligence Note, *supra* note 4 (mentioning, as examples of "spoofed" sites, "whitehouse.com" and "whitehouse.org").

tions that have the means to control financial information and Internet security.

The foregoing discussion demonstrates that there is no one solution at any one level that will solve the phishing problem. Stakeholders at each level can and must make greater efforts and institute new practices to prevent identity theft. Stakeholders among the levels also must collaborate with each other to find cross-level solutions. The organizations discussed in this Note are already moving in the right direction. The Anti-Phishing Working Group and Digital Phishnet, both of which combine law enforcement at the tertiary level and businesses at the secondary level, are already finding solutions. Secondary level organizations such as banks and ISPs are also working with consumers at the primary level to further educate them about ways they can protect themselves from identity theft scams such as phishing. While the phishing problem may never be solved, with these efforts it could remain more of an annoyance than a true cybercrime threat.