I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

RASHA ALMAHROOS*

Phishing for the Answer: Recent Developments in Combating Phishing

Abstract: This note discusses some legal implications of Phishing. First, it provides an introduction on Phishing and its variants. Then it discuss various efforts to combat Phishing, ranging from consumer education, private sector efforts, and law enforcement. Lastly, the article details recent legislative developments concerning Phishing at both the federal and state levels.

Phishing, also known as brand spoofing, is one of the most rapidly growing scams and methods of identity theft on the Internet today. Although comprehensive statistics on Phishing are hard to find, recent data indicates that the incidence of Phishing is growing and has increasingly become a matter of concern in the United States and the rest of the world. The Anti-Phishing Working Group ("APWG"), a global pan-industrial and law enforcement association focused on eliminating the identity theft and fraud that results from Phishing, issues reports on worldwide Phishing activity trends. The APWG's most recent report, published on November 2007, details an exponential growth in Phishing attacks.

* Rasha AlMahroos is a Juris Doctor candidate at The Ohio State University Moritz College of law. She obtained her Bachelors degree in Economics and Middle East Studies from the University of Virginia in August 2004. The author would like to thank Katy K. Liu, a 2007 graduate of the Ohio State University Michael E. Moritz College of Law.

I. INTRODUCTION–PHISHING: DEFINITION AND OVERVIEW

A. WHAT IS PHISHING?

Phishing refers to a method used by identity thieves to acquire personal information (e.g., names, passwords, Social Security numbers and credit card details) by using fraudulent e-mail messages that appear to originate from a legitimate business.[1] The term Phishing[2] originates from the analogy that the fraudster uses e-mails as bait to fish for profitable personal information from an unsuspecting sea of Internet users.[3] A typical Phishing attack utilizes the following steps:

1. The Phisher sends an e-mail that appears to originate from a legitimate business. Phishers usually achieve this by using familiar trademarks, tradenames and other common corporate identifiers.

2. The Internet Service Provider delivers the e-mail—which operates as bait—to an unsuspecting Internet user. The e-mail typically creates a false sense of urgency by informing the user that there is a problem with his or her account. The e-mail then requests personal information from the user in order to validate the account.

3. The recipient enters personal information or clicks on a phony website that mimics the appearance of the organization mentioned in the e-mail.

---

[1] Scot M. Graydon, *Phishing and Pharming: The New Evolution of Identity Theft*, 60 CONSUMER FIN. L.Q. REP. 335, 336 (2006).

[2] Phishing is spelled with "ph" instead of "f" to allude to "Phone Phreaking," a form of hacking popular in the 1970s that "used electronics to hack into telephones and get free calls." Microsoft, Pharming: Is Your Trusted Web Site a Clever Fake?, Jan. 3, 2007, http://www.microsoft.com/protect/yourself/phishing/pharming.mspx.

[3] Graydon, *supra* note 1, at 337.

4. The Phisher uses the information to commit identity theft and/or fraud.[4]

Although the incidence of Phishing has increased recently, it has been around for several years. Recent Phishing scams differ from their earlier counterparts in their levels of sophistication. While older Phishing e-mails were easily identifiable due to spelling, grammatical, and typographical errors, today's Phishing e-mails look legitimate. Moreover, current spyware technology allows Phishers to take advantage of software security flaws in order to avoid fraud and spam filters.[5] One form of spyware even allows the fraudulent URL to replace the actual URL in the victim's address bar by installing a fake address bar.[6] The fake address bar remains in the victim's computer and permits the Phisher to monitor the victim's Internet activity and access the information the victim sends and receives.[7]

B. SPEAR PHISHING, PHARMING, AND VISHING: MODERN FORMS OF DECEPTION WITH DEEP ROOTS

Generally, Phishing attacks are indiscriminate, relying on spam to target a large number of Internet users. However, over the past few years, Internet fraudsters have grown increasingly sophisticated and are using more targeted forms of Phishing to steal information from victims.

---

[4] NAT'L CONSUMERS LEAGUE, A CALL FOR ACTION 5 (2006), http://www.nclnet.org/news/2006/Final%20NCL%20Phishing%20Report.pdf.

[5] Jennifer Lynch, *Identity Theft in CyberSpace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259, 269 (2005).

[6] *Id.*

[7] *Id. See* Matthew Broersma, *Barkleys Scam Email Exploits New IE Flaw*, ZDNet UK, Jan. 12, 2004, http://news.zdnet.co.uk/security/0,1000000189,39119033,00.htm. "Customers of Barclays and other UK banks have been targeted by fraud emails that exploit a recently discovered vulnerability in Internet Explorer allowing attackers to disguise Web addresses, according to security experts. The Barclays scam email appears to come from the bank, and directs customers to a site posing as Barclays' online banking Web site, ibank.barclays.co.uk. The scam site then asks people to enter their banking details. Other scam emails appearing during the weekend also used this technique, known as 'phishing', along with the same IE bug. The organisations targeted include Citibank, Lloyds and PayPal."

1. SPEAR PHISHING

The term Spear Phishing describes an attack that targets a specific group of individuals.[8] Spear Phishers send e-mails that appear legitimate "to a specifically identified group of Internet users, such as certain users of a particular product or service, online account holders, employees or members of a particular company, government agency, organization, group, or social networking website."[9] Because the e-mail appears to come from a source that is trusted by the recipient, the request for personal information may appear more plausible and legitimate.

2. PHARMING

Pharming, also called Domain Spoofing, is a more sophisticated form of Phishing that uses trojan horse programs that compromise the user's computer or Domain Name System ("DNS") server to reroute Internet users from the Internet site they desire to view to an illegitimate site that mimics the legitimate site.[10] The user then enters his or her personal information into the database of the illegitimate website.

Pharming attacks are on the rise as savvy Internet users and companies have become more cautious about responding to Phishing attacks. Pharming is particularly dangerous because the end users are not aware of the attack; it does not require the user to follow a link to a fraudulent e-mail message. Instead, the attack occurs at the infrastructure level by compromising the user's computer. Thus, even the most careful Internet users may become victims of Pharming.[11]

---

[8] Microsoft, Spear Phishing: Highly Targeted Scams, Sept. 18, 2006, http://www.microsoft.com/protect/yourself/phishing/spear.mspx.

[9] BINATIONAL WORKING GROUP ON CROSS-BORDER MASS MKTG. FRAUD, REPORT ON PHISHING 8 (2006), http://www.usdoj.gov/opa/report_on_phishing.pdf.

[10] Polly Samuels McLean & Michelle M. Young, *Phishing and Pharming and Trojans–Oh My!*, 19 UTAH B.J. 28, 32 (2006).

[11] Graydon, *supra* note 1, at 343.

3. VISHING

In 2006, Vishing, also known as Voice Phishing, emerged as a twist on traditional Phishing.[12] Vishing is a technique that combines Internet and telephone resources to capture personal information.[13] In the typical Vishing scam, a customer receives a fraudulent e-mail message purporting to be from a bank or an e-commerce site such as eBay. The message states that the customer's account is disabled and that the customer must contact the account source to fix the problem. A telephone number is provided and the customer is told to call the number and provide personal account information.[14] Vishing is problematic because it takes advantage of inexpensive Internet technology such as Voice-over-Internet-Protocol, to emulate common bank-customer conduct in which customers are encouraged to call their bank and authenticate information.[15]

C. THE HARMFUL EFFECT OF PHISHING AND THE IMPACT ON ITS VICTIMS

Phishing scams have an adverse effect on individuals, companies, and the Internet as a whole. On an individual level, Phishing leads to direct financial loss. Phishers use an individual user's identity to withdraw money from the individual's account or open a new account under the individual's name. According to a survey by Gartner, Inc., 3.6 million Americans lost money due to Phishing in the twelve months ending in August 2007 compared to 2.3 million the previous year.[16] Although the average loss per individual decreased from $1,244 in 2006 to $886 in 2007, the number of victims increased, leading to a total loss of $3.2 billion.[17] Given the rise in Phishing

---

[12] *See* Herb Weisbaum, *'Vishing' Scams Use Your Telephone to Hook You*, MSNBC.COM, Aug. 1, 2006, http://www.msnbc.msn.com/id/14138614.

[13] Wikipedia, Vishing, http://en.wikipedia.org/wiki/Vishing (last visited Jan. 31, 2008).

[14] Weisbaum, *supra* note 12.

[15] BINATIONAL WORKING GROUP ON CROSS-BORDER MASS MKTG. FRAUD, *supra* note 9, at 10.

[16] Gartner is an information technology research and advisory company. *See* Press Release, Gartner, Gartner Survey Shows Phishing Attacks Escalated in 2007; more than $3 Billion Lost to These Attacks (Dec. 17, 2007), http://www.gartner.com/it/page.jsp?id=565125.

[17] *Id.*

activity in the past few years, it is very likely that these losses will increase annually.

Despite the adverse effects that Phishing has on individual Internet users, companies are the main victims of Phishing as they bear the majority of the direct financial loss that results from Phishing attacks.[18] Federal Deposit Insurance Corporation ("FDIC") regulations limit consumer liability for unauthorized transactions in their bank or credit card accounts to fifty dollars.[19] This means that the targeted institution is forced to absorb the remaining financial loss. In addition, companies targeted by Phishers also suffer harm to their goodwill and brand reputation.

> The criminals' abuse of the brand's reputation has immeasurable effects on marketing campaigns and customer confidence. The [P]hisher's use of the targeted companies' trademarked images and good names can also cause residual problems for consumers who may continue to associate the negative effects of the scam with the company. Victims may lose confidence in the company and wish to discontinue doing business there–a situation analogous to a reluctance to keep putting money in a bank that continues to be robbed.[20]

Phishing attacks also have a negative effect on the growth of Internet commerce generally. A 2006 consumer survey by Informa Research Services indicates that Phishing and other Internet-related scams have led to a loss in consumer confidence in the Internet marketplace.[21] Among several findings, the survey shows that 55% of consumers completely or strongly agreed with the statement that "Internet-based financial transactions are safe and secure," representing a 15% decrease from 2003.[22] The survey indicated that 67% of online consumers are very concerned about identity theft and

---

[18] Lauren L. Sullins, *"Phishing" for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft*, 20 EMORY INT'L L. REV. 397, 402 (2006).

[19] *Id.* at 402–03.

[20] *Id.* at 403.

[21] *Consumer Confidence in the Safety and Security of Internet Banking Continues to Decline According to Informa Research Services*, INFORMA RESEARCH SERVS., Apr. 10, 2006, http://www.informars.com/news/04_10_06.html.

[22] *Id.*

fraud on the Internet, and only 40% believed that Internet-based financial transactions are more secure than telephone banking, down from 47% in 2003.[23] Phishing erodes the public trust in the Internet because it leads to uncertainty in the integrity of commercial and financial websites, and even the Internet's addressing system. Thus, consumers are less likely to use the Internet for business transactions.[24]

II. METHODS OF COMBATING PHISHING

In October 2005, the U.S. Government announced the success of "Operation Firewall," in which the United States Secret Service collaborated with law enforcement agencies in New Jersey, the United Kingdom, Canada, Belarus, Poland, Sweden, Ukraine, and the Netherlands[25] to apprehend key members of shadowcrew.com and carderplanet.com, "one of the largest illegal online centers for trafficking in stolen identity information and documents, as well as stolen credit and debit card numbers."[26] The operation resulted in the indictment of nineteen individuals in the United States and two in the United Kingdom.[27] Another investigation, "Operation Cardkeeper," conducted by FBI agents and Polish and Romanian law enforcement agencies, led to the arrest of seventeen individuals involved in a global identity theft ring.[28]

Although operations such as these are often highly successful, their impact on combating Phishing is limited and unlikely to lead to a resolution of the Phishing problem if relied upon alone. In general, Phishing, like other forms of cyber-crime, presents a problem for law enforcement officials since the Phisher is protected by the anonymity of the Internet. Hence, social norms, such as the likelihood of being

---

[23] *Id.*

[24] BINATIONAL WORKING GROUP ON CROSS-BORDER MASS MKTG. FRAUD, *supra* note 9, at 11.

[25] Press Release, Dep't of Homeland Sec'y, U.S. Secret Service's Operation Firewall Nets 28 Arrests (Oct. 28, 2004), *available at* http://www.ustreas.gov/usss/press/pub2304.pdf.

[26] Press Release, Dep't of Justice, Nineteen Individuals Indicted in Internet 'Carding' Conspiracy (Oct. 28, 2004), *available at* http://www.usdoj.gov/opa/pr/2004/October/04_crm_726.htm.

[27] *Id.*; *see also* Paul F. Roberts, *UK Phishers Caught, Packed Away*, EWEEK.COM, June 27, 2005, http://www.eweek.com/c/a/Security/UK-Phishers-Caught-Packed-Away/.

[28] Kim Zetter, *FBI Busts Credit Cyber Gang*, WIRED, Nov. 3, 2006, http://www.wired.com/science/discoveries/news/2006/11/72064.

labeled a criminal, that may deter potential offline criminals do not apply.[29] This anonymity means that the probability of getting caught is substantially lower. The average Phishing site remains active for three days.[30] Thus, by the time Internet users discover that they are victims of Phishing and inform law enforcement authorities, the fraudulent site has already disappeared from the Internet. In addition, the costs of Phishing and other forms of cyber-crime are significantly lower than their offline equivalents.[31] It is necessary for the government to collaborate with other groups, such as private business entities and potential victims, for anti-Phishing measures to be effective. In fact, some commentators even see "law enforcement as having only a narrow role today because 'code, market forces, and . . . [self-help measures] have eclipsed law as the major institutions of social control in cyberspace.'"[32]

This section will discuss recent methods used to combat Phishing and their relative successes. These methods can be divided into two levels of attack. The first level of attack is extra-legal and is primarily concerned with self-help methods employed by potential victims and private entities. These methods include consumer education and private sector responses. The second level of attack is legislative and involves federal and state level responses to the Phishing problem. Although most states classify Phishing as a criminal act, some states provide civil remedies to victims of Phishing. The success of both levels of attack is wholly dependent on the collaboration between law enforcement, consumer advocates, and private sector entities.

---

[29] "Computers make it easier for criminals to evade the constraints of social norms (through pseudonymity and removal from the physical site of the crime), legal sanctions (the probability of getting caught may be reduced for similar reasons), and monetary costs (because the resource inputs necessary to cause a given unit of harm are much lower)." Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1011 (2001).

[30] ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS: REPORT FOR THE MONTH OF NOVEMBER, 2007 (2008), http://www.antiphishing.org/reports/apwg_report_nov_2007.pdf.

[31] *See, e.g.*, Susan Maclean, *Internet Criminals are Stronger Than Ever*, BUS. EDGE, July 21, 2005, http://www.businessedge.ca/article.cfm/newsID/10118.cfm.

[32] Lynch, *supra* note 5, at 273 (quoting PETER GRABOSKY ET AL., ELECTRONIC THEFT: UNLAWFUL ACQUISITION IN CYBERSPACE 8 (2001)).

A. THE FIRST LEVEL OF ATTACK: CONSUMER EDUCATION AND PRIVATE SECTOR RESPONSES

The first level of attack involves self-help measures that potential victims and private entities can take to insulate themselves and their customers from Phishing attacks. Two of these measures—consumer education and private sector prevention measures—will be addressed in the following paragraphs. The third common self-help remedy, civil litigation, will be discussed in subsequent sections.

1. CONSUMER EDUCATION

According to an identity theft survey conducted by the Federal Trade Commission, "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.'"[33] Because attacks are dependent on the active response of the victim, education and awareness are particularly important and perhaps the most effective method in preventing Phishing attacks. It is impossible to successfully conduct a Phishing attack if the victim is unwilling to input his or her personal information. Additionally, educated consumers can serve as informants by making agencies and companies aware of existing attacks.[34] Thus, educated Internet users are at the first line of defense against Phishers.

Information on Phishing scams and methods of protection are readily available on the Internet. Many non-profit organizations, such as the Anti-Phishing Working Group ("APWG") and FraudWatch International focus on educating users on the dangers of online fraud. Both organizations' websites offer resources to victims of Phishing attacks while also attempting to prevent future attacks by educating consumers on Phishing and showing them ways to protect themselves.[35] The U.S. Government also plays a role in consumer education. The Department of Justice and the Federal Trade Commission websites have articles that discuss identity theft prevention techniques. For example, OnGuard Online, an FTC-

---

[33] SYNOVATE, FED. TRADE COMM'N–IDENTITY THEFT SURVEY REPORT 7 (2003), http://www.ftc.gov/os/2003/09/synovatereport.pdf.

[34] Sullins, *supra* note 18, at 426.

[35] *Id.* at 429.

maintained website, gives consumers several simple suggestions that will help them avoid becoming victims of a Phishing scam. These suggestions include:

- Not replying to e-mails or pop-up messages that ask for personal information and avoiding copying and pasting a link from the e-mail to a web browser;
- Not calling any number provided in the e-mail;
- Avoiding sending personal and financial information through e-mail; and
- Reviewing credit card and bank statements as soon as they are received to check for any unauthorized changes.[36]

The most ingenious method of educating consumers so far, however, has come not from these informational sites but from private companies that educate and warn their customers directly about the harm of Phishing. This method is promising because it relies on teaching the customer in context at the moment the risk of a Phishing attack appears.[37] Instead of depending on informational websites, these companies include warnings in their e-mails, websites and others tools used by their customers. Wells Fargo Bank, for example, has dedicated a section of its website to information helping its customers prevent identity theft and e-mail scams,[38] as has NatWest Bank[39] and CitiBank.[40] eBay provides its customers with an anti-Phishing tutorial and also allows customers to download the eBay Toolbar Account

---

[36] OnGuard Online, OnGuard Online–Phishing, http://onguardonline.gov/phishing.html (last visited Jan. 31, 2008).

[37] *See* NAT'L CONSUMERS LEAGUE, *supra* note 4, at 19.

[38] Wells Fargo Fraud Information Center, https://www.wellsfargo.com/privacy_security/fraud/ (last visited Jan. 31, 2008).

[39] NatWest, NatWest Personal Banking, http://www.natwest.com/global_options.asp?id=GLOBAL/SECURITY (last visited Jan. 31, 2008).

[40] Citi, E-mail Fraud & Security–Report a Spoof, http://www.citi.com/domain/spoof/reportspoof.htm (last visited Jan. 31, 2008).

Guard, which protects its customers' eBay account information.[41] EarthLink has developed a similar toolbar and reports that as a result, the cost per attack has fallen from a peak of $115,000 to little more than $40,000.[42] PayPal, on the other hand, interrupts its own logging screens periodically with a Phishing warning, forcing consumers to click through the warning before going to the main screen.[43]

Despite these efforts, there remains a need to devote more resources to consumer education. A report by the National Consumer League recommends using more substantial resources, such as traditional public service announcements on television, as well as on the Internet, and new tutorials that teach in context to broaden the reach of consumer education efforts.[44]

Although education and awareness do play an immense role in preventing Phishing attacks, they cannot eliminate Phishing on their own. Phishing techniques have become more sophisticated and harder to detect. In some methods, such as Pharming, the user can do very little to prevent an attack because the Phisher is able to compromise the user's computer, thus removing the necessity of active user input. Hence, other methods of combating Phishing are necessary to prevent these forms of attack.

2. PRIVATE SECTOR PREVENTION MEASURES

Since Phishing attacks are increasing in their regularity and sophistication, Internet users cannot and should not be expected to eliminate Phishing attacks on their own. Because the financial burden that results from Phishing ultimately falls on the private sector, the private sector has begun to play a more active role in the prevention of Phishing attacks.[45] In light of this financial burden, along with the potential negative impact on a company's goodwill and brand image,[46] an anti-Phishing strategy directly benefits companies by helping to

---

[41] eBay, Recognizing Spoof (Fake) eBay Websites, http://pages.ebay.com/help/confidence/isgw-account-theft-spoof.html (last visited Jan. 31, 2008).

[42] Alice Dragoon, *Foiling Phishing*, CSO MAG., Oct. 2004, http://www.csoonline.com/read/100104/phish.html.

[43] *Id.*

[44] THE NAT'L CONSUMERS LEAGUE, *supra* note 4, at 2.

[45] *See, e.g.*, THE ANTI-PHISHING WORKING GROUP, *supra* note 30.

[46] Sullins, *supra* note 18, at 403.

ensure that their customers remain confident in doing business with them online.

Private sector involvement is important because it involves prevention at the infrastructural level and thus regulates attacks at a more immediate level than other anti-Phishing measures. Software manufacturers and Internet Service Providers, such as Microsoft, have begun to use technology that detects fraudulent websites and e-mails at the infrastructural level, thus helping to "create an ecosystem that is secure by design."[47] Sender ID, an e-mail authentication technology developed by Microsoft, combats fraudulent return addresses on e-mails.[48] "Sender ID 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.'"[49] eBay uses software developed by WholeSecurity, an Internet security firm based in Texas, in its Internet toolbar to detect fake sites purporting to be connected to eBay and its subsidiary, PayPal. Microsoft and Visa also use the same program.[50] Cisco and Yahoo! have also collaborated with numerous industry players to develop DomainKeys Identified Mail specification ("DKIM"), a method of e-mail identification that provides ways to validate "a domain name identity that is associated with a message through cyrpographic authentication."[51] DKIM uses a mail transfer agent[52] to insert a DKIM-signature heading in every e-mail that is sent. When the e-mail is received, a receiving mail transfer agent validates the signature by retrieving the sender's information through the DNS. The technology offers end-to-end protection of e-mail messages.[53]

---

[47] THE NAT'L CONSUMERS LEAGUE, *supra* note 4, at 3.

[48] Lynch, *supra* note 5, at 287.

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

[50] Press Release, WholeSecurity Inc., Microsoft, eBAY, PayPal, and Visa Join WholeSecurity to Launch Phish Report Network, the Internet's First Global Anti-Phishing Aggregation Service (Feb. 14, 2005), *available at* http://news.thomasnet.com/fullstory/460528.

[51] DKIM.org, DomainKeys Identified Mail (DKIM), http://dkim.org (last visited Jan. 31, 2008).

[52] "A mail transfer agent is a computer program or software agent that transfers electronic mail messages from one computer to another." Wikipedia, Mail Transfer Agent, http://en.wikipedia.org/wiki/Mail_transfer_agent (last visited Jan. 31, 2008).

[53] Wikipedia, DomainKeys Identified Mail, http://en.wikipedia.org/wiki/DomainKeys_Identified_Mail (last visited Jan. 31, 2008).

Credit card issuers, banks, and other members of the financial services industry are also developing tools to combat Phishing attacks. The Internet Technology Assistance Corporation, sponsored by the Financial Services Roundtable, a consortium of the largest 150 financial services companies in the United States, operates the Identity Theft Assistance Center ("ITAC"), which helps consumer victims of identity theft restore their identities on behalf of its member companies.[54] Individual bank and credit card companies are looking into implementing better user and site authentication methods, such as multi-factor authentication, which requires more than a single password to establish a user's identity.[55]

Despite recent private sector efforts to combat Phishing, many analysts argue that the private sector is not doing enough. While it is true that the financial services industry is the industry sector most targeted by Phishers, with 94.4% of all attacks recorded in the month of July 2007 alone, some statistics indicate that there is in fact little financial incentive to prevent Phishing and other methods of identity theft.[56] For example, according to estimates by Mastercard and Visa, "annual total fraud losses due to identity theft represented only 1/10th of one percent of annual sale volume."[57] Instead, the incentive to combat Phishing comes from the risk of decreased consumer confidence. However, although the private sector is taking concerted, expansive action to combat Phishing as a result of this, statistics such as these indicate that the private sector requires a greater financial incentive to combat Phishing even more aggressively. Regulations that hold the private sector accountable for losses that result from Phishing and other methods of identity theft may provide such an incentive. Federal banking agencies have implemented such an incentive by requiring that member banks use methods other than single-factor authentication in transactions involving access to customer information or the movement of funds to other parties, and believe that:

---

[54] *See* Identity Theft Assistance Center, http://www.identitytheftassistance.org/ (last visited Jan. 31, 2008).

[55] *See* FED. FIN. INST. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT, http://www.ffiec.gov/pdf/authentication_guidance.pdf (last visited Jan. 31, 2008).

[56] THE ANTI-PHISHING WORKING GROUP, *supra* note 30.

[57] Lynch, *supra* note 5, at 291.

> [F]inancial institutions should conduct a risk assessment to identity the types and levels of risk associated with their Internet banking applications. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties.[58]

B. THE SECOND LEVEL OF ATTACK: LEGISLATIVE RESPONSES

Legislation provides the second level of attack. It aims to combat Phishing that cannot be prevented or resolved by consumer education and the private sector alone. Legislation acts in one of two ways: it either creates incentives to prevent Phishing from taking place or attacks Phishing after it has already occurred. The following section will discuss recent legislative developments at both the federal and state levels.

Legislation enacted to prevent Phishing faces several difficulties in enforcement. The first difficulty is due to a lack of resources. "Investigators in Law Enforcement Agencies . . . often lag behind cyber criminals in terms of their understanding of technology and the equipment at their disposal."[59] In addition, Phishing tends to be fragmented with different people—often in different countries—responsible for various aspects of a Phishing attack "such as providing 'how-to' instructions, helping to set up spoofed sites and sending e-mails and laundering the proceeds."[60] The greatest difficulty, however, is jurisdictional. Due to the multi-state and multi-national nature of cybercrime, state and federal law enforcement may be constrained by jurisdictional boundaries. This is exacerbated by the fact that some U.S. law enforcement agencies are prohibited by law from sharing investigable information with their foreign counterparts, as well as with the private sector. "Law enforcement agencies,

---

[58] FED. FIN. INST. EXAMINATION COUNCIL, *supra* note 55.

[59] THE NAT'L CONSUMERS LEAGUE, *supra* note 4, at 25.

[60] *Id.*

Internet [S]ervice [P]roviders and entities that have been spoofed may each have vital information about a [P]hishing incident, but there is no central repository that specifically contains information about [P]hishing and that is accessible to both government and the private sector."[61] These problems have been addressed on a multi-national level in the Council of Europe's Convention of Cybercrime, as well as on a national level by the U.S. SAFE WEB Act approved by Congress in December 2006. However, jurisdictional issues still remain a problem: the U.S. SAFE WEB Act cannot eliminate all jurisdictional barriers, especially those of personal jurisdiction,[62] and the Council of Europe's Convention on Cybercrime has only been ratified by nineteen countries.[63]

1. FEDERAL LEGISLATIVE EFFORTS

Legislation explicitly addressing Phishing has not yet been passed. However, there have been a few recent federal legislative efforts and developments over the past year that provide some tools to address the Phishing problem.

A. THE CAN-SPAM ACT OF 2003

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, otherwise known as the CAN-SPAM Act, established the first nationwide standard for commercial e-mail and requires the Federal Trade Commission to enforce its provisions.[64] Since the CAN-SPAM Act specifically prohibits the use of deceptive subject lines and fake headers in e-mail messages, it can be used to target Phishers.[65] The first person to be convicted under the provisions

---

[61] *Id.* at 25–26.

[62] *See, e.g.,* Katyal, *supra* note 29, at 1095 n.244.

[63] ALEXANDER SEGAR, SPECIAL SESSION, THE CONVENTION OF CYBERCRIME OF THE COUNCIL OF EUROPE: A FRAMEWORK FOR NATIONAL ACTION AND INTERNATIONAL COOPERATION AGAINST CYBERCRIME (May 14–15, 2007), http://www.itu.int/osg/csd/cybersecurity/pgc/2007/events/presentations/lunch-session-seger-C5-meeting-15-may-2007.pdf.

[64] 15 U.S.C. § 7711 (2008).

[65] Spamlaws.com, Enacted Legislation: CAN-SPAM Act of 2003, http://www.spamlaws.com/federal/summ108.shtml (last visited Jan. 31, 2008).

of the CAN-SPAM Act was Jeffrey Brett Goodin, who in January 2007:

> was found guilty of sending thousands of e-mails to America Online users under the guise of messages from AOL's billing department that prompted customers to send personal and credit card information. He then used the information to make unauthorized purchases, officials said.[66]

B. THE U.S. SAFE WEB ACT OF 2006

The Undertaking Spam, Spyware and Fraud Enforcement with Enforcers Beyond Borders Act, known as the U.S. SAFE WEB Act, was signed into law on December 22, 2006.[67] The Act enhances the Federal Trade Commission's ability to protect consumers from Phishing and other forms of fraud by improving its ability to share information and to conduct joint investigative efforts with foreign law enforcement agencies. It also enables the FTC to obtain monetary consumer redress in cases involving spyware, spam, and Internet fraud.[68]

---

[66] Brian Prince, *Man Found Guilty of Targeting AOL Customers in Phishing Scam,* PC MAG., Jan. 18, 2007, http://www.pcmag.com/article2/0,2704,2085183,00.asp.

[67] Melissa Campanelli, *US Web Safe Act Signed into Law,* DMNEWS, Jan. 3, 2007, http://www.dmnews.com/US-Safe-Web-Act-signed-into-law/article/94010/.

[68] Posting of Charlene Brownlee to Privacy and Security Law Blog, http://www.privsecblog.com/archives/spam-us-safe-web-act-of-2006.html (Dec. 13, 2006, archived). The following is a summary of the key provisions of the Act as prepared by the FTC:

- Broadening Reciprocal Information Sharing. Allows the FTC to share confidential information in consumer protection cases with foreign law enforcers.
- Expanding Investigative Cooperation. Allows the FTC and foreign law enforcement agencies to obtain investigative assistance from one another in combating these consumer issues.
- Increasing Information from Foreign Sources. Exempts information from foreign agencies from public disclosure laws, which will increase their sharing of information with the FTC.

C. THE I-SPY PREVENTION ACT OF 2007

The Internet Spyware Prevention Act of 2007 ("I-SPY Prevention Act"), introduced by Representatives Zoe Lofgren (D-CA) and Bob Goodlatte (R-VA), would address Phishing by criminalizing the collection of personal information through fraudulent means. Specifically, it would prohibit intentionally accessing a prohibited computer without authorization, or exceeding authorized access by causing a computer program or code to be copied onto the protected computer, and intentionally using the program or code:

- in furtherance of another federal criminal offense; or
- to obtain or transmit personal information with the intent to defraud or injure a person or cause damage to a protected computer; or to impair the security protection of that computer.[69]

- Enhancing Confidentiality of FTC Investigations. Prevents notifying subjects of investigations if they may be likely to destroy evidence or move assets offshore.
- Protecting Certain Entities Reporting Suspected Fraud and Deception. Protects entities from liability for voluntary disclosures to the FTC relating to suspected fraud and deception, increasing the likelihood of such disclosures from third parties.
- Allowing Information Sharing with Federal Financial and Market Regulators. Helps FTC track proceeds of fraud and deception sent through U.S. banks to foreign jurisdictions so they can be returned to victims.
- Confirming FTC's Remedial Authority in Cross-Border Cases. Avoids challenges to FTC jurisdiction issues and encourages the full range of remedies for U.S. consumer victims in foreign courts.
- Enhancing Cooperation between FTC and DOJ in Foreign Litigation. Permits the FTC to work with DOJ to increase the resources relating to FTC-related foreign litigation, such as freezing foreign assets and enforcing U.S. court judgments abroad.

See Press Release, Senate Comm. on Commerce, Sci. & Transp., Congress Approves U.S. SAFE WEB Act (Dec. 9, 2006), *available at* http://commerce.senate.gov/public/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=248704&Month=12&Year=2006.

[69] H.R. 744, 109th Cong. (2005), *available at* http://www.theorator.com/bills109/hr744.html.

In addition, the Act appropriates a sum of $10,000,000 to Department of Justice prosecutions needed to discourage Phishing. It would also add a new Section 1030(A) to Title 18 of the U.S. Code, criminalizing the unauthorized accessing of, or placement of software on, protected computers, and that it includes a "sense of Congress" provision stating that the Department of Justice should use the amendments in the Act to prosecute Phishing and Pharming scams, as well as crimes using spyware. The bill passed in the House, but the Senate has failed to act on it. Earlier versions of the proposed Act have been criticized because they contained regulations that might criminalize or control certain types of technology, thus chilling innovation. The new 2007 version avoids such excessive regulation and thus has a greater change of being passed.[70]

D. THE ANTI-PHISHING ACT OF 2005

The Anti-Phishing Act of 2005, introduced by Senator Patrick Leahy is, thus far, the only proposed legislation that focuses solely on Phishing as opposed to more general forms of cybercrime or spam.[71] The Anti-Phishing Act has yet to become law. On February 28, 2007, it was referred to the Senate Judiciary Committee and the House Sub-Committee on Crime, Terrorism, and Homeland Security.[72] There has been no activity regarding the Act since then.[73] The Act would impose, among other things, hefty criminal penalties on persons who create fake websites and send bogus e-mails in order to defraud customers.[74] Additionally, it gives law enforcement agencies the ability to prosecute Phishers before they obtain victims' financial information.[75] Thus, unlike existing laws, no harm to the victim is necessary in order to establish a case. Critics of the Anti-Phishing Act

---

[70] Frederick Lane, *Feds Fight Phishing and Pharming with I-Spy Bill*, CRM DAILY, May 23, 2007, http://www.crm-daily.com/story.xhtml?story_id=52492.

[71] Wikipedia, Phishing, http://en.wikipedia.org/wiki/Phishing (last visited Jan. 31, 2008).

[72] Anti-Phishing Act of 2005, S. 472, 109th Cong. (2005), *available at* http://www.govtrack.us/congress/bill.xpd?bill=s109-472.

[73] *Id.*

[74] *See* Anita Ramasastry, *The Anti-Phishing Act of 2004: A Useful Tool against Identity Theft*, FINDLAW, Aug. 16, 2004, http://writ.news.findlaw.com/ramasastry/20040816.html.

[75] *See* Grant Gross, *Anti-Phishing Act Pushes for 5 Years and $250,000 Fine*, INDUS. STANDARD, Apr. 4, 2005, http://archive.thestandard.com/internetnews/002819.php.

believe that the Act's focus on criminal penalties does very little to stop the spread of Phishing.[76] Legislation that creates incentives to combat Phishing may be more effective.[77]

E. THE COUNCIL OF EUROPE'S CONVENTION ON CYBERCRIME

The Council of Europe's Convention on Cybercrime ("Convention") is the first and only international treaty that deals explicitly with cybercrime.[78] The Convention was ratified by the United States in 2006.[79] Its main goal is to harmonize world-wide laws relating to cybercrime.[80] This is especially important since cybercrime is often international in its nature. However, since only nineteen out of a total possible number of forty-three countries have ratified the convention, its effectiveness in that regard is limited.[81] The Convention requires participating countries to adopt laws that address "computer intrusion, computer-facilitated fraud, child pornography and copyright infringement" as well as other forms of cybercrime.[82]

The Convention is controversial because it lacks a dual criminality requirement.[83] This means that the FBI may be required to investigate and monitor foreign crimes even if the perpetrators of the crime are

---

[76] *See* Jack M. Germain, *Will Antiphishing Legislation Be Effective?*, E-COMMERCE TIMES, Nov. 13, 2004, http://www.ecommercetimes.com/story/38006.html?welcome=1202258939.

[77] *See id.*

[78] CYBER SEC. INDUS. ALLIANCE, RATIFYING THE EUROPEAN CONVENTION ON CYBERCRIME 1 (2005), http://www.csialliance.org/publications/csia_whitepapers/CSIA_CoE_Convention.PDF.

[79] *Senate Approves Cybercrime Treaty*, COMPUTERWORLD, Aug. 4, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002214.

[80] Council of Europe, Summary of the Convention on Cybercrime, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (last visited Jan. 31, 2008).

[81] SEGAR, *supra* note 63.

[82] *Id.*

[83] Electronic Privacy Information Center, The Council of Europe's Convention on Cybercrime, http://www.epic.org/privacy/intl/ccc.html.

under no suspicion for the crime in the United States.[84] Although the United States has ratified the Convention, it may refuse cooperation in international cybercrime investigations if the investigations violate certain basic rights, such as the right to free speech.[85]

2. STATE LEGISLATIVE EFFORTS

During the past few years, states have begun to take a more concerted action against Phishing and have passed legislation specifically targeting Phishing. California, Texas, New Mexico, Virginia, and Arizona earn the distinction of being the first states to pass laws to combat Phishing in 2005.[86] Of the five states, only New Mexico and Virginia made Phishing a criminal offense.[87] The other three only provide for civil penalties.[88] All five states created new momentum in the anti-Phishing legislative arena and there has been a greater legislative effort to pass anti-Phishing laws since then. Unlike New Mexico and Virginia, recently enacted state legislation, with a few exceptions, mostly provide only civil penalties, which include injunctive relief and/or damages. All states that provide for civil relief allow the attorney general to bring a civil action, as well as owners of a webpage or trademark that are adversely affected.[89] Only Connecticut and Louisiana allow for aggrieved individuals to seek recovery.[90] Currently, only Connecticut and Utah have enacted laws that provide criminal penalties for Phishing, with Utah providing only criminal and not civil penalties.[91] The states vary in their exact

---

[84] Declan McCullagh & Anne Broache, *Senate Ratifies Controversial Cybercrime Treaty*, CNET NEWS.COM, Aug. 4, 2006, http://www.news.com/Senate-ratifies-controversial-cybercrime-treaty/2100-7348_3-6102354.html.

[85] *Senate Approves Cybercrime Treaty*, *supra* note 79.

[86] Nat'l Conference for State Legislatures, 2005 Phishing Legislation, www.ncsl.org/programs/lis/phishing05.htm (last visited Jan. 31, 2008).

[87] *Id.*

[88] *Id.*

[89] *See* N.Y. Gen. Bus LAW § 390-b (2007); TENN. CODE ANN. § 47-18-5204 (2007); CONN. GEN. STAT. ANN. § 53-454 (West 2007); LA. REV. STAT. ANN. § 51:2034 (2007); OKLA. STAT. ANN. tit. 15, §§ 776.8-776.12 (West 2007); ILL. COMP. STAT. ANN. 7/1-15 (2008).

[90] *See* CONN. GEN. STAT. ANN. § 53-454 (West 2007); LA. REV. STAT. ANN. § 51:2034 (2007).

[91] *See* CONN. GEN. STAT. ANN. § 53-454 (West 2007); UTAH CODE ANN. § 76-10-1801 (2007).

definition of Phishing, with some states providing a broader definition than others. The following section will discuss recently enacted anti-Phishing legislation.

A. CONNECTICUT

On October 1, 2006, Public Act No. 06-50, became effective.[92] The law prohibits a person from using the Internet or e-mail to solicit or induce another person to provide identifying information by pretending to be an online Internet business without the authority or approval of the business.[93] The law is one of the few of its kind: it provides for both civil and criminal penalties with a violation of the law considered a felony.[94] Moreover, unlike the majority of state anti-Phishing laws, Connecticut's law allows any person who is the target of Phishing activity to "file a civil action in superior court," [95] in addition to the attorney general. Additionally, the court may increase the damages awarded if it finds that the defendant "engaged in a pattern and practice" of Phishing activity.[96] The plaintiff may recover "actual damages or twenty-five thousand dollars, whichever is greater" for each Phishing violation.[97]

The law explicitly states that an "interactive computer service provider" will not be held liable for violating the law if the service provider "remove[s] or disable[s] access to an Internet web page or other online location that such provider believes in good faith is being used to engage" in Phishing activity.[98]

---

[92] CONN. GEN. STAT. ANN. § 53-454 (West 2007).

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Id.*

B. LOUISIANA

In 2006, the "Anti-Phishing Act of 2006" was signed into law.[99] It prohibits "any person, by means of a web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business."[100]

Like Connecticut and Tennessee, Louisiana is one of the few states that allows an aggrieved person to sue for damages.[101] The attorney general, Internet Service Providers ("ISPs"), and webpage or trademark owners who are adversely affected may also bring civil suits.[102] Damages vary based on the type of plaintiff.[103] For all actions, a court may increase the damages awarded if the defendant is

---

[99] Anti-Phishing Act of 2006, LA. REV. STAT. ANN. § 51 (2007).

[100] LA. REV. STAT. ANN. § 51:2033 (2007).

[101] § 51:2034.

[102] *Id.*

[103] *Id.* (see table summarizing damages)

Party	Remedies/Damages	Limitations
"A person who is engaged in the business of providing Internet access to the public, owns a web page, or owns a trademark that is adversely affected by" a violation of the Anti-Phishing Act of 2006.	"[T]he greater of actual damages or five hundred thousand dollars . . . ."	
"An individual who is adversely affected by" a violation of the Anti-Phishing Act of 2006.	"[T]he greater of three times the amount of actual damages or five thousand dollars per violation . . . ."	"[O]nly against a person who has directly violated" the Anti-Phishing Act of 2006.
"The attorney general or a district attorney in a parish where a violation [of the Anti-Phishing Act of 2006] occurs."	"[E]njoin further violations" of the Anti-Phishing Act of 2006 "and to recover a civil penalty of up to two thousand give hundred dollars per violation . . . ."	

found to have "engaged in a pattern and practice of violating" the law.[104] Like most states, Louisiana does not criminalize Phishing.[105]

Louisiana also enacted the "Louisiana Anti-Phishing Act" in 2006.[106] The Act prohibits the use of a webpage or e-mail messages to solicit personal information or induce a person to provide personal information.[107] Parties who may file an action for violation of the Louisiana Anti-Phishing Act are Internet Service Providers, owners of a webpage or trademark who are adversely affected, and the attorney general.[108]

All parties are entitled to "[s]eek injunctive relief to restrain the violator from continuing the violation" or recover monetary damages.[109]

C. UTAH

Utah's Governor signed Senate Bill 52 into law on March 13, 2006, and, on May 1, 2006, the law became effective.[110] Utah's anti-Phishing legislation is unique in that it only provides for criminal penalties.[111] Before Senate Bill 52, the Utah criminal code prohibited, and assigned criminal penalties to a person found guilty of, "devis[ing] any scheme or artifice to defraud another or to obtain from another money, property, or anything of value by means of false or fraudulent pretenses, representations, promises, or material omissions."[112] Senate Bill 52 adds a penalty of "a second degree felony when the object or purpose of the scheme or artifice to defraud is the obtaining of sensitive personal identifying information, regardless of the value."[113]

---

[104] *Id.*

[105] LA. REV. STAT. ANN. § 51:2033 (2007).

[106] §§ 51:2021–2025.

[107] §§ 51:2022–2023.

[108] § 51:2024.

[109] *Id.*

[110] UTAH CODE ANN. § 76-10-1801 (2007).

[111] *Id.*

[112] S.B. 52, 56th Leg., 2006 Gen. Sess., 2006 Utah Laws 120.

[113] § 76-10-1801

Personal identifying information includes a Social Security number, driver license number or other government issued identification number, financial account number, an automated or electronic signature, unique biometric data, or any other information that can be used to gain access to an individual's financial accounts or to obtain goods or services.[114] Senate Bill 52 did not alter the criminal code provisions that state that a perpetrator's intent is not considered when determining whether the perpetrator has engaged in fraud.[115]

D. NEW YORK

On June 7, 2006, the Governor of New York signed into law the "Anti-Phishing Act of 2006."[116] The Act defines Phishing as obtaining identifying information by misrepresenting oneself as a business.[117] Parties who may bring a civil action to seek injunctive relief and monetary damages include the attorney general, ISPs, and those owning a webpage or trademark, who are adversely affected by violations of the Anti-Phishing Act of 2006.[118] An individual adversely affected by Phishing may not bring a civil action.[119] If the defendant is "found to have engaged in a pattern and practice of violating" the Act, a court may enhance the damages awarded and award reasonable attorney's fees and court costs to the prevailing party.[120]

E. TENNESSEE

The Anti-Phishing Act of 2006 was signed into law in May 2006.[121] The Act prohibits persons from obtaining, recording,

---

[114] *Id.*

[115] *Id.*

[116] N.Y. GEN. BUS. LAW § 390-b (2007).

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] TENN. CODE ANN. §§ 47-18-5201–5205 (2007).

accessing or distributing identifying information from another person without his or her permission through the use of the Internet, e-mail, or any other form of electronic communication.[122] Any violation of the Act "shall be construed to be an unfair or deceptive act or practice affecting trade or commerce."[123]

Like the majority of legislation passed in other states, the Act provides for civil relief only. However, it also allows any person who suffers an ascertainable loss to seek relief, instead of only ISPs and owners of a webpage or trademark that are adversely affected.[124] The attorney general may also bring a civil action with a civil penalty of $2,500.[125]

F. OKLAHOMA

On April 17, 2006, the "Anti-Phishing Act," was signed into law.[126] The Act revises Oklahoma state law by amending statutes and adding several new sections.[127] The Act makes Phishing a violation of the Consumer Protection Act. The Act adds a section stating that a person may not create a webpage Internet domain name to misrepresent itself as a legitimate, online business and use the webpage "to induce, request, or solicit another person to provide identifying information."[128] Like anti-Phishing laws in the majority of states, only the following parties may bring an action for violations of the Anti-Phishing Act: (1) "[a] person engaged in the business of providing Internet access service to the public who is adversely affected"; and (2) "[a]n owner of a webpage or trademark who is adversely affected."[129] The plaintiff may seek injunctive relief,

---

[122] § 47-18-5203.

[123] § 47-18-5205.

[124] § 47-18-5204.

[125] *Id.*

[126] Mohamed Chawki, *Phishing in Cyberspace: Issues and Solutions*, COMPUTER CRIME RESEARCH CTR., Aug. 16, 2006, http://www.crime-research.org/articles/phishing-in-cyberspace-issues-and-solutions/2.

[127] OKLA. STAT. ANN. tit. 15, §§ 776.8–776.12 (West 2007).

[128] § 776.10.

[129] § 776.11.

monetary damages, or both.[130] For defendants who the court determines have engaged in a pattern of violating the Anti-Phishing Act, the court may enhance the damage award.[131] A defendant who is found liable must also pay the plaintiff reasonable attorney's fees and court costs.[132]

G. HAWAII

Hawaii takes a unique approach to anti-Phishing. Instead of providing for criminal and/or civil penalties, Hawaii created the Identity Theft Task Force[133] in 2006 to reduce electronic commerce based crimes.[134] The Identity Theft Task Force is required to: (1) identify the best practices to prevent identity theft; (2) establish a timetable for the removal of personal identifying information from public records in Hawaii; (3) review the current practices of other jurisdictions associated with the use and disclosure of government records containing Social Security numbers, the current volume and likely future increase or decrease in the volume of these government records, and the practicability of any proposed mandatory redaction from certain types of records or documents; and (4) identify and recommend solutions to Social Security number protection issues.[135]

H. ILLINOIS

The Anti-Phishing Act was signed into law in August 2007.[136] The Act makes it illegal to obtain identifying information through the Internet by acting as a business without the permission of that business.[137] Like other anti-Phishing legislation passed, the Act allows

---

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] The Identity Theft Task Force replaced the Anti-Phishing Task Force, which was established in 2005.

[134] Electronic Commerce; Identity Theft, H.B. 3244, 23d Leg. (Haw. 2006), *available at* http://www.capitol.hawaii.gov/session2006/bills/hb3244_cd1_.htm.

[135] *Id.*

[136] ILL. COMP. STAT. ANN. 7/1-15 (West 2008).

[137] *Id.*

the attorney general, ISPs, and owners of a webpage or trademark who are adversely affected to bring an action for a violation of this kind.[138] The plaintiff adversely affected may recover "the greater of three times the amount of actual damages or $5,000 per violation."[139] The attorney general may recover a civil penalty of $2,500 per violation.[140]

III. CONCLUSION

Phishing is one of the fastest growing scams and methods of identity theft on the Internet today. While it may never be completely eradicated, its threat and its effect on victims can be greatly reduced. In order to combat Phishing in a comprehensive manner, resources need to be focused on developing methods of attack that focus on consumer education, private sector cooperation, and legislative enforcement, and to increase cooperation between these three methods. There has already been a move in this direction. Both the federal government and an increasing number of states have passed legislation that aim to combat Phishing and other forms of identity theft. The private sector and consumer protection groups have devoted increasing resources to consumer education and other anti-Phishing measures. However, there is a need for more collaboration in order to develop more comprehensive solutions that will effectively reduce Phishing and its variants.

---

[138] *Id.*

[139] *Id.*

[140] *Id.*