PHISHING FOR ELDERLY VICTIMS: AS THE ELDERLY MIGRATE TO THE INTERNET FRAUDULENT SCHEMES TARGETING THEM FOLLOW

Eric L. Carlson

Internet usage is no longer limited to a young, tech-savvy subset of the population. As elderly people use the Internet in increasing numbers, the con artists who prey on them adapt their tactics accordingly. In this note, Eric Carlson explains why the elderly are especially susceptible to Internet fraud. He describes three fraudulent schemes regularly perpetrated against the elderly and the devastating effects they have on older Americans. While relevant legislation, prosecution of offenders, and education of the elderly all help to alleviate the occurrence of fraud, the problem persists. Mr. Carlson concludes that legislation and enforcement measures are helpful but insufficient to address the problem, and that society—including neighbors, family, and especially young, tech-savvy friends—has an obligation to help elderly people avoid falling victim to fraudulent Internet schemes.

Eric L. Carlson is Notes Editor 2006–2007, Member 2005–2006, The Elder Law Journal; J.D. 2007, University of Illinois, Urbana-Champaign; B.S. 2004, University of Illinois, Urbana-Champaign, College of Engineering.

The author would like to thank his parents, Stephen and Joanne Carlson, for their continued support and encouragement. Go Illini!

I. Introduction

To a large degree, the Internet is synonymous with a hip, tech-savvy, and young demographic. Heavily influenced by pop culture and the mainstream media, the modern-day Internet is typically characterized by young entrepreneurs, teenage hackers, bloggers, social networking Web sites, online gaming, and file-sharing. All things related to an older generation of Internet users are seemingly left out of the mix.

Because older generations have historically perceived computer-based technology to be overly complicated and the Internet difficult to access, the elderly have traditionally comprised a small fraction of the Internet-using population. However, the present day widespread availability of computing resources and the ubiquitous nature of the Internet have made this technology readily available to all demographics. Consequently, members of older generations are using the Internet with increasing frequency, and many of them become prime targets of fraudulent schemes against which they have no method of self-defense because of limited knowledge and scarce resources.

This note analyzes the aforementioned trend of Internet fraud perpetrated against the elderly. Specifically, Part II explores the relevant background by examining the explosive growth of the elderly demographic in America, the increasing presence of the elderly on the Internet, and reasons why the elderly are susceptible to fraud. Part III analyzes the recent surge in Internet fraud, specific fraudulent schemes that are of particular concern to the elderly, and various methods for dealing with the Internet fraud epidemic. Part IV argues that the most effective method for protecting the elderly from Internet fraud revolves around preemptive education. Further, Part IV emphasizes that education of this type must be creative and carefully designed to reach the elderly.

II. Background

A. Growing Elderly Population

The elderly population in the United States is growing at an astonishing rate. According to the most recent U.S. Census data, there are thirty-five million people sixty-five years of age or older living in

the United States.[1] This figure represents 12.4% of the total U.S. population.[2] The number of people sixty-five or older in the United States has increased more than ten times since 1900.[3] Moreover, the growth rate of the elderly population was much larger than the growth rate of the general population.[4] From 1900 to 1994, the population of people sixty-five years of age or older increased by a factor of eleven.[5] During the same time period, the population as a whole grew by a factor of only three.[6]

In 2011, the oldest members of the baby boomer[7] generation will begin to turn sixty-five,[8] and the sixty-five and older population is projected to double to seventy million by the year 2030.[9] Further, projections indicate that by the year 2030, 20% of all Americans will be sixty-five years of age or older.[10] This staggering growth is predominantly a result of significant increases in life expectancies.[11] Between 1900 and 1997, the life expectancy in the United States rose from 47.3 years to 76.5 years.[12]

B. Migration of the Elderly Demographic to the Internet

As the elderly population grows exponentially, so, too, does the presence of the elderly on the Internet. Older Americans are going

1. YVONNE J. GIST & LISA I. HETZEL, U.S. CENSUS BUREAU, WE THE PEOPLE: AGING IN THE UNITED STATES 1 (2004), *available at* http://www.census.gov/prod/2004pubs/censr-19.pdf.

2. *Id.*

3. FED. INTERAGENCY FORUM ON AGING RELATED STATISTICS, OLDER AMERICANS 2000: KEY INDICATORS OF WELL-BEING, http://www.agingstats.gov/chartbook2000/population.html (last visited Aug. 18, 2006) [hereinafter OLDER AMERICANS 2000]. The United States is a relatively young country when compared with other developed nations. In many industrialized nations, people ages sixty-five and over constitute 15% or more of the total population. *Id.*

4. Frank B. Hobbs, U.S. Census Bureau, The Elderly Population, *available at* http://www.census.gov/population/www/pop-profile/elderpop.html (last visited Aug. 18, 2006).

5. *Id.*

6. *Id.*

7. This term is used to refer to the generation of people that were born shortly after the conclusion of World War II.

8. OLDER AMERICANS 2000, *supra* note 3.

9. *Id.*

10. *Id.*

11. *See* U.S. Info., Embassy of the U.S., Copenhagen, Den., Intro to the U.S., http://www.usembassy.dk/IntroUS/AmericanSociety/Demographics.htm (last visited Aug. 18, 2006).

12. *Id.*

online in record numbers.[13] According to the Pew Internet Project, 59% of people between the ages of fifty and sixty-four and 22% of people age sixty-five and older became Internet users by August 2003, and those numbers will most likely continue to increase.[14] Other research indicates that 31% of the sixty-five and older population has gone online,[15] and of these, 46% go online every day.[16] Furthermore, "[o]ver the next decade, as baby boomers and other adults get older, the proportion of seniors using the Internet is likely to increase dramatically."[17] This increase is poised to take place as 70% of Americans ages fifty to sixty-four have used the Internet and 64% have Internet access in their homes.[18] According to estimates by the American Association of Retired Persons (AARP), "50 to 60 million adults 50-plus will be online by 2011."[19] This statistic is significant, as it suggests that more than half of the fifty-plus age group will soon be online.[20]

The Internet has become "increasingly attractive to all segments of the population as a medium for everyday information-gathering, communication, and commercial activity,"[21] and the elderly are no ex-

13. *Internet Fraud Hits Seniors: As Seniors Venture into the Web, the Financial Predators Lurk and Take Aim: Hearing Before the U.S. S. Spec. Comm. on Aging*, 108th Cong. 78 (2004) [hereinafter *Internet Fraud Hits Seniors*] (statement of Sen. Larry Craig).

14. *Id.* at 12 (statement of Dave Nahmias, Deputy Assistant Att'y Gen., Criminal Div., U.S. Dep't of Justice).

15. VICTORIA RIDEOUT ET AL., KAISER FAMILY FOUND., E-HEALTH AND THE ELDERLY: HOW SENIORS USE THE INTERNET FOR HEALTH INFORMATION 1 (2005), *available at* http://www.kff.org/entmedia/upload/e-Health-and-the-Elderly-How-Seniors-Use-the-Internet-for-Health-Information-Key-Findings-From-a-National-Survey-of-Older-Americans-Survey-Report.pdf [hereinafter ELDERLY INTERNET SURVEY].

16. *Id.*

17. *Id.* at 3.

18. *Id.* at 1.

19. Andrew Wind, *Computer, E-mail Training Help Elderly Man Stay Sharp*, WATERLOO CEDAR-FALLS COURIER, Feb. 13, 2006, *available at* http://www.wcfcourier.com/articles/2006/02/13/news/top_story/e858aa6e4ff4e3ed862571140051d0fd.txt.

20. *Id.* European countries such as Germany are also witnessing this trend. *See, e.g.*, Press Release, Fed. Statistical Office of Germany, Internet Use by Elderly People Grows Above Average (Apr. 18, 2005), http://www.destatis.de/presse/englisch/pm2005/p1790024.htm ("As reported by the Federal Statistical Office, the use of the [I]nternet in the German population . . . is further increasing. This is true not only of young people but also . . . of the elderly: 22% of those aged over 54 went online in the first quarter of 2004, while in 2002 the figure was just 16%. For comparison: [a]mong the total population from the age of ten, 58% used the [I]nternet. The increase among elderly people (+38%) is clearly above the growth rate for the population aged 10 and over (+26% in 2002).").

21. *Internet Fraud Hits Seniors*, *supra* note 13, at 12 (statement of Dave Nahmias, Deputy Assistant Att'y Gen., Criminal Division, U.S. Department of Justice).

ception. Older Americans utilize the Internet to access healthcare information, keep in touch with family and friends, seek entertainment, and engage in commercial transactions.[22] The Kaiser Family Foundation reports that the Internet serves as a resource for health information for one in five Americans ages sixty-five years or older.[23] Further, the Kaiser Family Foundation reports that for Americans ages fifty to sixty-four, "the [I]nternet has actually surpassed TV and books as a source of 'a lot' of health information."[24] As far as staying in touch with family and friends, about a third of seniors claim that the Internet is "an important part of their life that they wouldn't want to do without."[25] More than half of seniors assert that the Internet and e-mail make it "'a lot' easier for them to stay in touch with family and friends."[26]

Additionally, older Americans are turning to the Internet for entertainment.[27] A recent survey found that 19% of video gamers are fifty years of age or older, as compared with 9% in 1999.[28] According to Carolyn Rauch, a senior vice president of the Entertainment Software Association trade group, today's baby boomers are much more technologically savvy than previous generations of elderly, and they are more inclined to take gaming with them as they age.[29] Older players are interested in interacting with other players across the world via the Internet and seem to be "attracted to games involving strategy and historical simulations."[30]

22. ELDERLY INTERNET SURVEY, *supra* note 15.
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.*
27. *See generally* Patrick J. Kiger, *Generation Xboxers: Computer Game Developers Are Targeting an Older Slice of the Market*, AARP BULL., Feb. 2006, *available at* http://www.aarp.org/bulletin/yourlife/gen_xboxers.html.
28. *Id.*
29. *Id.*
30. *Id.* Two examples of computer games that target an older slice of the market are *Railroad Tycoon*, "a historical simulation in which players pretend to be early-1900s industrialists," and *Brothers in Arms*, a World War II simulation. *Id.* One fifty-six-year-old man, Kevin O'Hare, reports that he typically goes online around six o'clock to play *Everquest*, a massively multiplayer online role-playing game. *Id.* O'Hare further explains that it is not unusual for him to remain on the Internet and play the game well past midnight. *Id.*

C. The Elderly Are Attractive Targets for Fraud in General

Historically, the elderly serve as prime targets for con artists who seek illicit financial gain.[31] Studies indicate that up to five million seniors annually are victims of some type of financial fraud.[32]

Based on its extensive experience in investigating fraud, the Federal Bureau of Investigation (FBI) has identified five prominent reasons why the elderly are frequently targets of fraud.[33] First, the elderly are more likely to be in a desirable economic position.[34] Persons ages fifty-years-old and up control approximately 70% of the nation's household wealth, and they are projected to be in control of approximately $10 trillion in assets within the next ten years.[35] The elderly often possess large "nest eggs" that sit dormant in bank accounts, ripe for the taking.[36] Also, many elderly people have large amounts of equity in their homes and excellent credit ratings.[37]

Second, the elderly "come from a generation where business was often conducted on a handshake alone."[38] Those who were raised in the early to middle 1900s were generally taught to be polite and trusting[39] and are thus less likely than younger generations to become suspicious during unscrupulous transactions.[40] Third, the elderly are also less likely to report fraud that criminals perpetrate against them.[41] Even if they are savvy enough to recognize that they have been victimized, many elderly people are too ashamed to report incidents of fraud.[42] In addition, "an elderly victim may not report the crime because he or she is concerned that relatives [or friends] may come to the conclusion that the victim no longer has the mental capacity to

31. *See Old Scams—New Victims*: *Breaking the Cycle of Victimization: Hearing Before the U.S. S. Spec. Comm. on Aging*, 109th Cong. 2–3 (2005) [hereinafter *New Victims*] (statement of Sen. Herb Kohl).
32. *Id.*
33. FBI, Fraud Target: Senior Citizens, http://www.fbi.gov/majcases/fraud/seniorsfam.htm (last visited Aug. 18, 2006) [hereinafter FBI].
34. *Id.*
35. *Internet Fraud Hits Seniors*, *supra* note 13 (statement of David Jevans, Chairman, Anti-Phishing Working Group).
36. FBI, *supra* note 33.
37. *Id.*
38. *New Victims*, *supra* note 31 (statement of Sen. Herb Kohl).
39. FBI, *supra* note 33 ("The con-man will exploit these traits knowing that it is difficult or impossible for these individuals to say 'no' or just hang up the phone.").
40. *Id.*
41. *Id.*
42. *Id.*

take care of his or her own financial affairs."[43] Moreover, elderly people may not know where to report the crime.[44]

Fourth, the FBI has found that the elderly often make poor witnesses.[45] In most cases, it takes people of all ages many weeks or months to realize that they have been victimized by fraud.[46] This significant delay, combined with memory lapses and diminished cognitive abilities, makes it difficult for elderly witnesses to precisely and accurately recall detailed information crucial to an investigation.[47] Finally, the elderly are natural targets for some of the most common fraudulent schemes that deal with seemingly "too good to be true" investment scams and "miracle" medical products.[48] "In a country where new cures and vaccinations for old diseases have given every American hope for a long and fruitful life, it is not so unbelievable that the products offered by these con-men can do what they say."[49] Thus, the elderly are more prone to put suspicions behind them and buy into a fraudulent scheme.

III. Analysis

A. Internet Fraud Is on the Rise

The Internet is quickly becoming the most prominent vehicle for conducting fraud.[50] Elaborate schemes for committing mass fraud are nothing new in modern society. Fraudulent schemes historically used standard mail or the telephone as the preferred medium for exploiting victims. Telemarketers defraud consumers of billions of dollars annually,[51] and "[m]ost Internet fraud has clear antecedents in telemarket-

43. *Id.*
44. *Id.*
45. *Id.*
46. *Id.*
47. *Id.* ("[T]he elderly victim will not be able to supply enough detailed information to investigators such as: How many times did the fraudster call? What time of day did he/she call? Did he provide a call back number or address? Was it always the same person? Did you meet in person? What did the fraudster look like? Did he/she have any recognizable accent? Where did you send the money? What did you receive if anything and how was it delivered? What promises were made and when? Did you keep any notes of your conversations?").
48. *Id.*
49. *Id.*
50. *See* Leda Mouallem, *Oh No, Grandma Has a Computer: How Internet Fraud Will Take the Place of Telemarketing Fraud Targeting the Elderly*, 42 SANTA CLARA L. REV. 659, 672–73 (2002).
51. *Id.* at 660.

ing fraud. What is different about Internet fraud is the size of the potential market, and the relative ease, low cost, and speed with which a scam can be perpetrated."[52] Scam artists are now using this new medium and the opportunities that it presents to "[pitch] old scams to new victims, perpetuating a cycle of victimization."[53]

Research supports the assertion that Internet fraud is on the rise. One statistic that is particularly telling explains the steep increase in Internet fraud complaints filed with various government agencies. In 2001, the Internet Crime Complaint Center (IC3) received only 49,711 complaints,[54] but in 2004, the IC3 received 207,449 complaints.[55] According to the National Internet Fraud Watch Information Center, the average Internet fraud victim in 2004 lost $895, up from $527 in 2003.[56] Between January 2005 and June 2005, a further increase was observed as the average Internet fraud victim lost $2579.[57]

B. The Internet Is an Effective Vehicle for Fraud

The Internet is an effective vehicle for committing fraud, as it caters to the execution of transient, global, and high-tech schemes. The Federal Trade Commission (FTC) reports that the Internet "is the latest draw for opportunistic predators who specialize in fraud"[58] and presents "a host of novel challenges" that stretch government re-

52. Rolando Berrelez, Assistant Regional Dir. of the Midwest Region of the FTC, Prepared Statement: Fraud Against Seniors (Aug. 10, 2000), http://www.ftc.gov/os/2000/08/agingtestimony.htm.

53. *New Victims*, *supra* note 31, at 1 (statement of Sen. Gordon H. Smith).

54. NAT'L WHITE COLLAR CRIME CTR. & THE FBI, IFCC 2001 INTERNET FRAUD REPORT 4 (2001), *available at* http://www.ic3.gov/media/annualreport/2001_IFCCReport.pdf.

55. NAT'L WHITE COLLAR CRIME & THE FBI, IC3 2004 INTERNET FRAUD-CRIME REPORT 3 (2004), *available at* http://www.ic3.gov/media/annualreport/2004_IC3Report.pdf.

56. Nat'l Internet Fraud Watch Info. Ctr., Internet Scams Fraud Trends 2004 (2004), http://www.fraud.org/2004-internet%20scams.pdf.

57. Nat'l Internet Fraud Watch Info. Ctr., Internet Scams Fraud Trends January–June 2005 (2005), http://www.fraud.org/internet/internet_scams_halfyear_2005.pdf.

58. *On-Line Fraud and Crime: Are Consumers Safe? Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 107th Cong. 21 (2001) [hereinafter *Internet Fraud Hearing*] (testimony of Eileen Harrington). "The Federal Trade Commission (FTC) is the federal government's primary consumer protection agency. . . . [Its] jurisdiction extends over nearly the entire economy, including business and consumer transaction on the Internet." *Id.* at 20.

sources thin.[59] The Internet is particularly conducive to fraud for several reasons.

First of all, the Internet allows con artists to expand the scope and size of traditional scams. "A colorful, well-designed Website imparts a sleek new veneer to an otherwise stale fraud[,] and the reach of [the] Internet allows an old-time con artist to think—and act—globally."[60] The new frontier of cyberspace breathes life into antiquated scams, such as those that purport to repair credit, work-at-home scams, and pyramid schemes.[61] "The Internet provides an efficient way to reach countless new fraud prospects around the world, and to funnel funds more efficiently . . . from the victims to the scammers."[62] Second, the Internet allows scams to become increasingly high-tech.[63] "Although most Internet fraud stems from traditional scams, the number of schemes [that] ingeniously [exploit] new technology is multiplying. These are the most insidious schemes because they feed on the public's fascination with . . . new technology."[64] With the aid of readily available software, criminals are able to cloak themselves in anonymity and evade law enforcement.[65] In order to keep up with the criminals, government agencies are forced to engage in vigorous Internet training programs[66]—a continual challenge due to limited resources.

Third, the Internet serves as an effective vehicle for fraud due to the ephemeral nature of online scams, many of which spread rapidly and then quickly disappear. "Using anonymous emails, short-lived [Web sites], and falsified domain name registrations, many fraud operators are able to strike quickly, victimize thousands of consumers in

59. *Id.* at 7 ("The Commission faces a host of novel challenges in its efforts to combat fraud and deception online.").

60. *Id.* at 24.

61. *See id.* Pyramid schemes are an example of a classic fraud whose size and scope are magnified by the Internet. When a pyramid scheme uses the Internet as a vehicle, "the victims are more numerous, the fraud operator's financial 'take' is much greater, and the defense is typically well-funded and fierce when the FTC brings suit to stop a pyramid scheme operating online." *Id.* at 24.

62. *Id.* at 24.

63. *Id.* at 25–27.

64. *Id.* at 25.

65. *Id.* at 27 ("One hallmark of Internet fraud is the ability of perpetrators to cover their tracks and mask their locations and identities.").

66. *Id.* For example, "[r]ecognizing that most of its attorneys and investigators need to be Internet savvy, the [Federal Trade] Commission has hosted beginner and advanced Internet training seminars and held session on new technology, investigative techniques, and Internet case law." *Id.* at 25.

a short period of time, and disappear . . . without a trace."[67] Finally, effective remedies to Internet fraud are difficult to achieve in the global online market.[68] Criminals who commit Internet fraud often conduct all or part of their operations abroad,[69] rendering many of them both legally and practically beyond the reach of the FTC and U.S. courts.[70] Further, as international law has become exceedingly complex, recognition of civil judgments from country to country is severely limited.[71] "Even if the [FTC was] to bring an action and obtain a judgment against a foreign firm that has defrauded U.S. consumers, the judgment might be challenged in the firm's home country, and the ability to collect any consumer redress might be frustrated."[72]

C. The Elderly Are Particularly Susceptible to Internet Fraud

Recent statistics provide evidence that the elderly are particularly affected by the rise in Internet fraud. In 2004, Consumer Sentinel,[73] the complaint database developed and maintained by the FTC, received more than 645,000 consumer fraud and identity theft complaints.[74] Consumers ages fifty and older filed 145,895 of these complaints, representing 26% of all complaints received.[75] Of these complaints, the FTC deemed 39,100 of them "Internet-related."[76] Consumers fifty and older who filed a complaint lost an average of

67. *Id.* at 27.
68. *Id.* at 28.
69. *Id.* For example, in *FTC v. J.K. Publications*, No. 99-000-44ABC (C.D. Cal. 1999), after the FTC obtained a $37.5 million verdict against a scam operator defendant, the defendant moved millions of dollars of misappropriated funds to the Cayman Islands, Liechtenstein, and Vanuatu. *Id.* The FTC never recovered this money in full. *Id.*
70. *Id.*
71. *Id.*
72. *Id.*
73. Consumer Sentinel is a complaint database maintained by the FTC. Consumer Sentinel collects information regarding fraud and identity theft from more than 150 organizations across the nation. Leading organizations who contribute to the Consumer Sentinel Database include the FBI, the Department of Defense, the U.S. Postal Inspection Service, the National Consumers League, and the Internet Crime Complaint Center. FTC, FRAUD AND IDENTITY THEFT COMPLAINTS RECEIVED BY THE FEDERAL TRADE COMMISSION FROM CONSUMERS AGE 50 AND OVER 3 (2005), *available at* http://aging.senate.gov/public/_files/ftc.pdf [hereinafter FRAUD COMPLAINTS].
74. *Id.* at 4.
75. *Id.*
76. A complaint is deemed "Internet-related" if "it concerns an Internet product or service, the company initially contacts the consumer via the Internet, or the consumer responds via the Internet." *Id.* at 10.

$1280 to fraud.[77] These statistics show that a wide variety of older Americans are victimized by fraud. Older Americans who are entering the final stages of their lives and baby boomers who are just beginning to face the issues of older generations have fallen prey to Internet scams.

D. Specific Internet Schemes Perpetrated Against the Elderly

1. PHISHING

In 2003, the FBI labeled phishing as "the hottest, and most troubling, new scam on the Internet."[78] Phishing is the name that Internet subcultures have given to a particular type of e-mail-based fraud that tricks victims into divulging their personal information.[79] "Phishing isn't really new—it's a type of scam that has been around for years and in fact predates computers. Malicious crackers did it over the phone for years and called it social engineering. What is new is its contemporary delivery vehicle—spam and faked Web pages."[80]

Fundamental to phishing schemes are carefully crafted, forged e-mail messages. A phishing scheme typically begins with a mass mailing of forged e-mail messages.[81] On its face, the e-mail appears to be a legitimate e-mail from a reputable bank, Internet service provider, e-commerce company, or government agency.[82] "To appear credible and to attract the recipient's attention, the e-mail uses [a] company's logos and trademarks and employs 'scare tactics' such as threats of ac-

77. *Id.* People between the ages of fifty and fifty-nine filed 71% of all Internet-related complaints filed by individuals over the age of fifty. *Id.* People ages sixty to sixty-nine were responsible for filing 23% of these complaints. *Id.* People ages seventy and older filed 7% of all complaints. *Id.*

78. *Internet Fraud Hits Seniors*, *supra* note 13, at 78 (statement of David Jevans, Chairman, Anti-Phishing Working Group).

79. "The term 'phishing' comes from the analogy that Internet scammers are using email lures to 'fish' for passwords and financial data [in] the sea of Internet users. The term was coined in the 1996 timeframe by hackers who were stealing America Online (AOL) accounts by scamming passwords from unsuspecting AOL users." *Id.* at 77. "'Ph' is a common hacker replacement for 'f', and is a nod to the original form of hacking in the early 1970's known as 'phone phreaking.'" *Id.* Many "hackers" or "cyber criminals" use 'ph' in the spelling of otherwise common words. *See id.* at 78.

80. Russel Kay, *Phishing*, COMPUTERWORLD, Jan. 19, 2004, *available at* http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=89096&pageNumber=1.

81. *See id.*

82. *Id.*

count closure."[83] These e-mails appear to be from an entity with which one might do business and that might solicit the verification or update of personal information such as account numbers, passwords, social security numbers, and credit card numbers.[84] The subject lines of phishing e-mails contain such seemingly legitimate messages as "Update Your Online Banking Records," "Ameritrade Online Application," "Notice From VISA," or "Citibank Alert Service."[85] The body of a typical phishing e-mail is usually similar to the example below:[86]

> Dear Citibank Customer
>
> We were unable to process the recent transactions on your account. To ensure that your account is not suspended, please update your information by clicking here.
>
> If you have recently updated your information, please disregard this message as we are processing the changes you have made.
>
> Citibank Customer Service
>
> Citibank Alerting Service
>
> Citibank [alert@citibank.com][87]

In addition, a phishing e-mail provides the recipient with a link to a fake Web site that is meticulously designed to look identical to the authentic site of the business which the e-mail purports to represent.[88] The Web site utilizes a seemingly legitimate online form to gather personal information that is immediately sent to the cyber criminal's anonymous e-mail account.[89] The unsuspecting victim, meanwhile,

83. Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259, 265–66 (2005).

84. Kay, *supra* note 80.

85. Anti-Phishing Working Group, Phishing Archive, http://www.antiphishing.org/phishing_archive.html (last visited Aug. 18, 2006) [hereinafter Phishing Archive].

86. *Id.* Other prevalent phishing schemes involve e-mails from popular commerce Web sites such as eBay. *Id.* One such phishing e-mail that was in heavy circulation in March of 2005, purported to be from eBay and threatened account termination. Anti-Phishing Working Group, eBay—'eBay: Account Violate User Agreement' (Mar. 7, 2005), http://www.antiphishing.org/phishing_archive/03-07-05_Ebay/03-07-05_Ebay.html. The authentic looking e-mail body opened as follows: "We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please click here and re-enter your account information." *Id.*

87. Anti-Phishing Working Group, Citibank—'Citibank Alerting Service' (Nov. 10, 2004), http://www.antiphishing.org/phishing_archive/11-10-04_Citibank/11-10-04_Citibank.html.

88. *See* Lynch, *supra* note 83, at 259–60.

89. *See id.* at 267.

remains under the false impression that a legitimate business entity is merely verifying his or her personal information.[90]

Phishing scams are constantly evolving to become more sophisticated and effective.[91] Advanced phishing e-mails and Web sites use technologies such as e-mail spoofing, proxy servers, DNS hijacking, DNS poisoning, and crimeware.[92] These elaborate schemes are alarmingly successful, capable of deceiving even seasoned Internet users. E-mails sent as part of a phishing scam yield an average positive response rate of between 1% and 5% of all recipients.[93] This statistic is staggering considering a spammer's ability to send out literally hundreds of thousands of e-mails in a matter of minutes with the aid of readily available software.[94]

While phishing scams have negative consequences that reverberate throughout the Internet community as a whole, they are of particular concern to the elderly. The elderly "make appealing targets, and should be particularly careful of phishing attacks, because they have potentially the most to lose."[95] As the elderly are members of the newest demographic to venture into cyberspace, they are naturally the least educated about the dangers and intricacies of phishing fraud.[96] Their lack of Internet savvy combined with the strong financial incentives to target them make phishing a serious menace to the elderly.

2. IDENTITY THEFT

Phishing is just one method of engaging in online identity theft, a crime of the utmost concern for elderly Internet users. A digital identity thief can first set up a phishing scam to obtain the personal identifying information of hundreds or thousands of people.[97] After

90. *See id.* at 260.

91. *Internet Fraud Hits Seniors*, *supra* note 13, at 78 (statement of David Jevans, Chairman, Anti-Phishing Working Group).

92. *See* ANN L. KEITH, NAT'L CTR. FOR STATE COURTS, TRENDS IN IDENTITY THEFT 2 (2005), *available at* http://www.ncsconline.org/WC/Publications/Trends/2005/PripubIDTheftTrends2005.pdf; Phishing Archive, *supra* note 85.

93. *Internet Fraud Hits Seniors*, *supra* note 13, at 78 (statement of David Jevans, Chairman, Anti-Phishing Working Group).

94. *See* Lynch, *supra* note 83, at 263.

95. *Internet Fraud Hits Seniors*, *supra* note 13, at 78 (statement of David Jevans, Chairman, Anti-Phishing Working Group).

96. *See id.*

97. Lynch, *supra* note 83, at 262–64 ("In close to the same 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.").

obtaining sufficient identifying information, the criminal "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 [victim's] bank account, or use a [victim's] information when arrested for a crime."[98] Identity theft affects victims in more ways than simply depriving them of wealth.[99] Victims of identify theft often report various nonmonetary harm such as "emotional distress from feeling personally violated by the theft, being harassed by creditors and collection agencies for debts that they did not incur, being turned down for a loan or new account, or even being arrested for crimes committed by someone else in their name."[100]

There are many examples of elderly people becoming mercilessly victimized by identity theft. In one particularly infamous instance, Jeffrey Grover, the former owner of a small Florida Internet service provider company, stole the identities of numerous elderly people.[101] One of Grover's victims was Nelson Doubleday, the wealthy president of Doubleday Publishing Company and an instrumental figure in the 1980 purchase of the New York Mets.[102] In Grover's testimony before the U.S. Special Committee on Aging, he explained that by using techniques that are "lengthy and technical," in just a few hours he was able to obtain the full name, address, date of birth, social security number, previous addresses, and information on any vehicles and property that his victims owned.[103] Once Grover obtained this information, it was easy for him to go "online, apply for a credit card [in his victim's name,] and be approved within a few minutes."[104] Further, Grover was able to essentially control the bank accounts of his victims—Mr. Doubleday included.[105]

98. *Id.*
99. *See id.*
100. *Id.* (discussing how identity theft may destroy credit ratings to the point where victims can no longer obtain loans, and in the worst cases, victims often have to spend up to 200 hours to repair their credit history and reestablish their good name).
101. *Internet Fraud Hits Seniors*, *supra* note 13, at 33–34 (statement of Jeffrey Grover, Inmate, Federal Correctional Institute, Yazoo City, Mississippi).
102. *Id.* at 4. In January of 1980, Doubleday Publishing Company bought the New York Mets franchise for $21.1 million.
103. *Id.*
104. *Id.*
105. *Id.* ("I would then run a complete credit report from any one of the online credit reporting agencies and find out who you had credit accounts with. From

While identity theft is a concern to the Internet community as a whole, senior Internet users are especially at risk.[106] Of all the identity theft complaints the FTC received in 2004, 26% came from people fifty years of age or older.[107] This statistic is especially compelling because of the elderly demographic's relatively limited presence on the Internet. The FTC states that "the most striking difference between [identity theft victims] under 50 and those over 50 [is] the greater prevalence of older consumers that had new credit accounts opened in their names."[108] Typically, elderly people are less likely than younger people to make major purchases, such as buying a house, car, or other luxury item.[109] Because of this, they are less likely to review their credit reports or the terms of their home refinancing, which "means that [the elderly] may be less likely than some younger homeowners and consumers to detect that they have become identity theft victims" and to detect that new credit accounts have been opened in their names.[110] Moreover, the elderly tend to be more dependent than other segments of the population on caregivers "such as relatives, medical staff, service personnel, and oftentimes, complete strangers,"[111] and "[s]uch dependency 'increases their vulnerability to certain schemes involving identity theft.'"[112] Despite the grave risk identity theft poses

there I could then tap into your bank account, providing that I had the right circumstances.").

106. *Id.*

107. FRAUD COMPLAINTS, *supra* note 73, at 5.

108. *New Victims*, *supra* note 31, at 9. "While such complaints represented 16.5 percent of all ID theft complaints for the general population, 19.6 percent of complaints from older consumers involved this type of identity fraud. Our identity theft survey found that this form of 'New Account' fraud was more difficult for consumers to discover, more costly, and posed greater challenges for recovery." *Id.* at 15–16 (statement of Lois C. Greisman, Associate Director of the Division of Planning and Information, Bureau of Consumer Protection, FTC); *see* Kay, *supra* note 80.

109. *Internet Fraud Hits Seniors*, *supra* note 13, at 18 (statement of Dave Nahmias, Deputy Assistant Att'y Gen., Criminal Division, U.S. Department of Justice).

110. *Id.*

111. Erin Leigh Sylvester, *Identity Theft: Are the Elderly Targeted?*, 3 CONN. PUB. INT. L.J 313, 321 (2004), *available at* http://www.law.uconn.edu/journals/cpilj/contents/archives/vol3/sylvester.pdf.

112. *Id.* (quoting *Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves: Hearing Before the Subcomm. on Social Security of the H. Ways & Means Comm. and the Subcomm. on Immigration, Border Security & Claims of the H. Comm. on the Judiciary*, 107th Cong. 57 (2002) (testimony of Robert Bond, Deputy Special Agent in Charge, Financial Crimes Division, U.S. Secret Service)).

to the elderly, "[o]ne survey determined that more than one-third of adults over sixty . . . did not know what identity theft is."[113]

3. ONLINE AUCTION FRAUD

Another form of fraud plaguing the Internet is online auction fraud. Online auction sites[114] serve as fertile ground for fraud because "[u]nlike traditional auctions, where the parties or their representatives are in the room with the offered merchandise, online auction sites use the Internet to conduct a virtual auction where the parties never meet and the buyer has no opportunity to examine the offered goods."[115] In the context of online auctions, fraud occurs both during the bidding process and after it has concluded.[116] One common form of fraud that takes place during the bidding process is known as "shill bidding," a tactic that artificially inflates the price of the auctioned item by placing one or more false bids with no intention of purchasing the item.[117] "Typically, parties employ different user names to make these fraudulent bids, bidding on either their own or their co-conspirators' offered items."[118] Detecting shill bidding and other forms of collusive bidding is extremely time-consuming and complex.[119]

Once an auction has closed, there exist two forms of fraud that are commonly perpetrated.[120] "The first and most common scenario . . . typically occurs when a seller fails to deliver the promised goods after the buyer has paid in full."[121] A similar fraud occurs when the seller delivers the item on which the buyer bid, but because of ma-

113. *Id.* at 332. This is an especially telling statistic considering that less than one-fifth of younger adults did not know what the crime of identity theft was. *Id.*

114. Examples of online auction Web sites include www.ebay.com, www.ubid.com, auctions.yahoo.com, and auctions.amazon.com.

115. Miriam R. Albert, *E-Buyer Beware: Why Online Auction Fraud Should Be Regulated*, 39 AM. BUS. L.J. 575, 582 (2002).

116. *Id.* at 581–82.

117. *Id.* at 589–91.

118. *Id.* at 589.

119. *Id.* at 590 ("Tracing collusive bidding is time-consuming, involving hours of sifting through and matching up myriad bidding histories and user feedback. Because of cost considerations and storage capacity issues, auction records may be expunged from an online auction site after a set number of days. This may affect the viability of any investigation into shill bidding or other forms of collusion, as the bidding record retention period may not be long enough to allow investigators to uncover shill bidders who spread out their fraudulent bids.").

120. *Id.* at 591.

121. *Id.* As its description implies, this scam is referred to as "failure to deliver."

terial misrepresentations made by the seller, the received item is different from what the buyer expects.[122]

Online auction fraud "is becoming an increasingly pervasive problem due to the lack of meaningful consumer protection in the form of appropriate regulation and enforcement . . . as well as the dearth of consumer education efforts."[123] Auction fraud accounted for approximately 29% of all Internet-related complaints recorded by people age sixty and older.[124] Moreover, online auction fraud ranked third in a list of the top fifteen product or service complaints reported by seniors.[125]

E. Measures to Curtail Internet Fraud

1. LEGISLATIVE MEASURES

To counter the rise in Internet fraud, certain members of Congress have proposed anti-phishing legislation. On July 9, 2004, Senator Patrick Leahy (D-Vt.)[126] introduced Senate Bill 2636, the Anti-phishing Act (APA) of 2004,[127] to the U.S. Senate.[128] If enacted, the APA would introduce two new crimes into the U.S. Code.[129] First, subsection (a) of the APA would regulate Web-site phishing:

> [W]hoever knowingly, with the intent to carry on any activity which would be a Federal or State crime of fraud or identity theft—(1) creates or procures the creation of a website or domain name that represents itself as a legitimate online business, without the authority or approval of the registered owner of the actual website or domain name of the legitimate online business; and (2) uses that website or domain name to induce, request, ask, or solicit any person to transmit, submit, or provide any means of

122. *Id.*
123. *Id.* at 592.
124. *Internet Fraud Hits Seniors*, *supra* note 13, at 48 (statement of Howard Beales, Director, Bureau of Consumer Protection, FTC).
125. *Id.*
126. *See* Patrick Leahy Biographical Sketch, (2005), http://leahy.senate.gov/biography/sketch05index.html. Leahy "was elected to the United States Senate in 1974 and remains the only Democrat elected to this office from Vermont." *Id.* Additionally, "Leahy is the Ranking Member of the Judiciary Committee and is a senior member of the Agriculture and Appropriations Committees. [Leahy] ranks seventh in seniority in the Senate." *Id.* Leahy is sometimes referred to as the cyber senator for his "Net-friendly" enthusiasm and leadership in the realm of Internet-related law. *Id.*
127. Anti-phishing Act of 2004, S. 2636, 108th Cong. (2004).
128. Matt Brady, *Anti-Phishing Bill Likely to Be Reintroduced in Congress*, 109 NAT'L UNDERWRITER LIFE & HEALTH 5, 27 (2005).
129. *See* S. 2636, § 3.

> identification to another; shall be fined under this title or imprisoned up to five years, or both.[130]

Second, subsection (b) of the APA would regulate e-mail phishing:

> [W]hoever knowingly, with the intent to carry on any activity which would be a Federal or State crime of fraud or identity theft—(1) falsely represents itself as being sent by a legitimate online business; (2) includes an Internet information location tool that refers or links users to an online location on the World Wide Web that falsely purports to belong to or be associated with such legitimate online business; and (3) induces, requests, asks, or solicits a recipient of the electronic mail message directly or indirectly to provide, submit, or relate any means of identification to another; shall be fined under this title or imprisoned up to five years, or both.[131]

David Jevans, chairman of the Anti-Phishing Working Group,[132] contends that while the APA would allow law enforcement officials to stop phishing schemes at earlier stages than before, the chief value of the APA is premised on deterrence.[133] "The focus of the bill . . . is . . . preventing more individuals from engaging in phishing rather than trying to deal with those already involved."[134]

Despite the apparent need for the APA, Congress has been slow to pass the bill. The APA of 2004 never went to hearing before the Senate or the House of Representatives and consequently was never put to a vote.[135] The APA of 2004 went no further than being referred to the Senate Committee on the Judiciary for review.[136] The two-year term of the 108th Congress elapsed before Congress could take additional action with respect to the APA of 2004.[137] On February 28, 2005, Senator Leahy reintroduced his phishing legislation to the 109th Congress.[138] This new bill, referred to as the Anti-Phishing Act of 2005, is virtually identical to the failed APA of 2004.[139] As Leahy introduced

130. *Id.* According to Leahy, the intent requirement was included in light of First Amendment concerns. Brady, *supra* note 128, at 27. Specifically, the intent requirement seeks to protect parody and political commentary. *Id.*

131. S. 2636, § 3(b).

132. David Jevans and the Anti-Phishing Working Group collaborated with Senator Leahy on drafting the APA. Brady, *supra* note 128, at 29.

133. *Id.*

134. *Id.*

135. *Id.* at 27.

136. *Id.* at 29.

137. *Id.* (noting that the failure of the APA of 2004 to win passage was not a reflection of the substance of the bill, but was purely a time issue and due to "the circumstances of 2004").

138. 151 CONG. REC. S1804 (daily ed. Feb. 28, 2005) (statement of Sen. Leahy).

139. *See infra* note 142. The APA of 2005 is cosponsored in the Senate by Senator Charles Schumer (D-N.Y.). 151 CONG. REC. S1804 (daily ed. Feb. 28, 2005)

the APA of 2005 to the Senate, he emphasized that phishing schemes undermine the confidence Americans have in the Internet.[140] Furthermore, Leahy insisted that the APA of 2005 was necessary, as "traditional wire fraud and identity theft statutes are not sufficient" to combat phishing.[141] In spite of this renewed push for anti-phishing legislation, Congress has again been slow to react. In the Senate, on February 28, 2005, the APA of 2005 was referred to the Senate Committee on the Judiciary for review.[142] The Committee on the Judiciary has yet to take further action.[143] In the House, the APA of 2005 awaits review in the Subcommittee on Crime, Terrorism, and Homeland Security of the House Committee on the Judiciary.[144] It remains unclear when, and if, Congress will move forward in effectuating the passage of the APA of 2005.

Aside from the APA, Congress has been active in crafting other legislation aimed at eliminating Internet fraud. On July 15, 2004, President George W. Bush signed the Identity Theft Penalty Enhancement Act into law, establishing the federal criminal offense of aggravated identity theft.[145] This law mandates an additional prison sentence of two years for aggravated identity theft convictions.[146] This two-year prison term is imposed on top of the punishment for other

(statement of Sen. Leahy). The technical name of the APA of 2005 in the Senate is Senate Bill 472. *See infra* note 144. Additionally, the APA of 2005 was introduced to the House of Representatives on March 3, 2005. *Id.* In the House, the APA of 2005 is technically known as House Bill 1099. *Id.*

140. 151 CONG. REC. S1804 (daily ed. Feb. 28, 2005) (statement of Sen. Leahy).

141. *Id.* ("Some phishers . . . can be prosecuted under wire fraud or identity theft statutes, but often these prosecutions take place only after someone has been defrauded. For most of these criminals, that leaves plenty of time to cover their tracks. It has been reported that the average phishing website is active on the Internet for less than six days. Moreover, the mere threat of these attacks undermines everyone's confidence in the Internet. When people cannot trust that websites are what they appear to be, they will not use the Internet for their secure transactions. Traditional wire fraud and identity theft statutes are not sufficient to respond to phishing . . . .").

142. The Library of Congress, THOMAS, S. 472, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:SN00472:@@@X (last visited Aug. 18, 2006) [hereinafter THOMAS, S. 472].

143. *See id.*

144. The Library of Congress, THOMAS, H.R. 1099, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:HR01099:@@@X (last visited Aug. 18, 2006).

145. The substance of this Act is codified at 18 U.S.C.A. § 1028A (West 2000 & Supp. 2006). *See also* George W. Bush, U.S. President, Remarks by the President at Signing of Identity Theft Penalty Enhancement Act (July 15, 2004), http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html ("The law I sign today will dramatically strengthen the fight against identity theft and fraud.").

146. *Id.*

crimes[147] that stem from the perpetrated identity theft.[148] Additionally, the Internet Spyware (I-SPY) Prevention Act of 2005 (ISPA) is currently working its way through Congress.[149] On March 23, 2005, the House passed the ISPA, and it was subsequently sent to the Senate for consideration.[150] The ISPA's congressional findings emphasize that "[t]wo particularly egregious types of [Internet] schemes are the use of spyware and phishing scams."[151] In general, the ISPA criminalizes the act of intentionally causing a computer program to be copied onto a protected computer and then intentionally using that computer program in furtherance of a federal offense or the collection of personal data.[152]

A handful of states have decided to take anti-phishing legislation into their own hands.[153] For example, to explicitly combat the phishing threat, Virginia has updated its Computer Crimes Act.[154] This legislation "makes it a felony to use a computer or computer network to entice another person to divulge personal financial or identifying information by means of a knowing misrepresentation as to the identity

147. Such crimes include wire fraud, 18 U.S.C.A. § 1343 (West 2000 & Supp. 2006), and mail fraud, 18 U.S.C.A. § 1341 (West 2000 & Supp. 2006).

148. *Id.*

149. *See generally* The Library of Congress, THOMAS, H.R. 744, http://thomas.loc.gov/cgi-bin/bdquery/z?d109:HR00744:@@@X (last visited Aug. 18, 2006).

150. *Id.*

151. H.R. 744, 109th Cong. (2005).

152. *Id.* Under subsection (a), "[w]hoever intentionally accesses a protected computer without authorization, or exceeds authorized access to a protected computer, by causing a computer program or code to be copied onto the protected computer, and intentionally uses that program or code in furtherance of another Federal criminal offense shall be fined under this title or imprisoned not more than 5 years, or both." *Id.*

153. *See generally* ARK. CODE ANN. § 4-111-103 (West 2005) (stating that "[n]o person shall engage in phishing"); CAL. BUS. & PROF. CODE § 22948 (West 2005) (California's Anti-Phishing Act of 2005 provides that "[i]t shall be unlawful for 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"); TEX. BUS. & COM. CODE ANN. § 48.001 (Vernon 2006) (The Texas Anti-Phishing Act prohibits the fraudulent creation of a Web page that is represented as a legitimate online business in order to solicit identifying information from a third party); VA. CODE ANN. § 18.2-152.1 (West 2006) (The Virginia Computer Crimes Act provides for certain remedies for the misappropriation of identifying information and the distribution of such information).

154. *See generally* VA. CODE ANN. § 18.2-152.1 (West 2006); Press Release, Commonwealth of Va., Office of the Att'y Gen., Jagdmann Hails Signing of Anti-Phishing Legislation into Law (Mar. 29, 2005) (on file with The Elder Law Journal).

or authority of the person requesting the information."[155] Also, the updated Virginia legislation reduces the damage threshold with respect to computer trespass from $2500 to $1000.[156]

Legislation specifically tailored to the Internet is undoubtedly an important tool in the fight against online fraud, but the effectiveness of such legislation is severely limited by the fast-paced and global nature of the Internet.[157] The Internet allows criminals to spread their criminal activity across numerous countries and engage in near-anonymous communications. As a result, the enforcement of Internet legislation faces formidable hurdles, such as finding the perpetrator of an Internet-based crime, obtaining personal jurisdiction over any found perpetrators, and enforcing any resulting penalty or judgment.[158]

2. PROSECUTORIAL AND ENFORCEMENT METHODS

To combat the threat of Internet fraud, the federal government has orchestrated numerous aggressive enforcement operations. One such program is Operation E-Con, "a coordinated initiative focusing on significant Cyber Crime activity both in the United States and a number of other countries across the Globe."[159] The operation is designed to show that those who participate in Internet fraud will suffer real-world consequences.[160] In 2003, as part of Operation E-Con, the U.S. Attorney's Office for the District of Maryland indicted two "phishers" for "devising and executing a scheme to lure unsuspecting

155. *Id.*
156. *Id.*
157. *See* Robert Louis B. Stevenson, *Plugging the "Phishing" Hole: Legislation Versus Technology*, 2005 DUKE L. & TECH. REV. ¶ 35 (2005), http://www.law.duke.edu/journals/dltr/articles/PDF/2005DLTR0006.pdf.
158. *Id.* ¶ 14.
159. INTERNET FRAUD COMPLAINT CTR., OPERATION E-CON, EXECUTIVE SUMMARY, http://www.ic3.gov/media/initiatives/econbrief.pdf (last visited Aug. 18, 2006). Operation E-Con is jointly coordinated by the U.S. Department of Justice, the FBI, the U.S. Postal Inspection Service, the U.S. Secret Service, and the FTC. *Id.* Also, a number of state organizations play a crucial role assisting in ongoing fraud investigations. *Id.*
160. *See* Press Release, U.S. Dep't of Justice, Fact Sheet, Operation E-Con: Cracking Down on Internet Crime (May 16, 2002), http://www.usdoj.gov/opa/pr/2003/May/03_crm_302.htm ("Those who participate in Internet Fraud and Abuse have learned their illegal activities have real-world consequences."). As of May 2002, Operation E-Con "executed over 70 search and seizure warrants that have led to 130 arrests and convictions and over $17 million in seizures and recoveries." *Id.*

bank customers to 'spoofed' bank websites."[161] In another E-Con phishing bust, the U.S. Attorney's Office for the Western District of Pennsylvania indicted a criminal defendant for charges of conspiracy, bank fraud, and access device fraud.[162] The criminal defendant in this particular case ran a scheme by which he would obtain the Social Security numbers of elderly victims, with which he would then apply for bank loans over the Internet.[163] The federal government reinforced the notion that Internet fraud has "real-world" consequences when it sentenced the defendant in this case to twenty-one months in prison and charged him with $25,000 in restitution.[164] Furthermore, "[t]he Department of Justice has brought a number of criminal prosecutions against individuals who engage in the fraudulent sale of drugs and medical devices that may put senior citizens at risk."[165] In one particular instance, a college student used the e-mail address Hydrocodone@anywhereUSA.com to post fake messages on the Internet site www.healthboards.com.[166] In these postings, the student made fake offers to sell drugs such as morphine, skelaxin, and percocet.[167] The FBI uncovered this scheme in an undercover operation, and the student was subsequently indicted.[168]

As a follow up to Operation E-Con, the federal government initiated Operation Web Snare, "a collaborative nationwide enforcement operation directed at major forms of online economic crime and other cybercrimes."[169] This operation "involved coordination among 36 U.S.

161. *Internet Fraud Hits Seniors*, *supra* note 13, at 18 (statement of Dave Nahmias, Deputy Assistant Att'y Gen., Criminal Division, U.S. Department of Justice) (stating that one of these criminals, who pled guilty to bank fraud charges and wire fraud charges, is now awaiting federal sentencing).

162. *Id.* at 19.

163. *Id.*

164. *Id.* Additionally, in Operation Cyber Sweep, a follow-up operation to Operation E-Con, the U.S. Attorney's Office for the Eastern District of Virginia obtained a guilty plea from a defendant who engaged in a phishing operation to solicit the user names and passwords of America Online users. *Id.* This defendant was sentenced to forty-six months of imprisonment. *Id.*

165. *Id.* at 22.

166. *Id.* at 22–23.

167. *Id.*

168. *Id.* This defendant was caught after an undercover FBI agent had extensive e-mail contact with the defendant regarding the potential purchase of a variety of drugs. *Id.*

169. Press Release, U.S. Dep't of Justice, Justice Department Announces Operation Web Snare Targeting Online Fraud and Crime (Aug. 26, 2004), http://www.usdoj.gov/opa/pr/2004/August/04_crm_583.htm. Specifically, Operation Web Snare targets "crimes including identity theft, fraud, counterfeit software, computer intrusions, and other intellectual property crimes." *Id.* "The

Attorneys' offices nationwide, the Criminal Division of the Department of Justice, 37 of the FBI's 56 field divisions, 13 of the Postal Inspection Service's 18 field divisions, [and] the FTC, together with a variety of other federal, state, local and foreign law enforcement agencies."[170] As a part of Operation Web Snare, various government agencies have identified more than 150,000 victims with estimated losses of more than $215 million.[171]

In one case, the U.S. Department of Justice brought criminal proceedings against R. Mark Pentrack in Utah.[172] Pentrack was the mastermind of a scheme in which he used the Internet to sell car parts he neither possessed nor had any intention of delivering to their rightful buyers.[173] Ultimately, "Pentrack was sentenced to more than 11 years in prison as a result of his guilty pleas to mail fraud, misuse of a Social Security number, attempted destruction of evidence, and making a false statement in connection with an Internet fraud scheme."[174]

The FTC also plays an active role in seeking out online scams and the criminals who mastermind them.[175] One such FTC program is called "Surf Days."[176] An FTC official explained how Surf Days work:

> On a typical Surf Day, Commission staff and personnel from our law enforcement partners—often state attorneys general, sister federal agencies or private organizations like the Better Business Bureau—widely "surf" the Internet for a specific type of claim or solicitation that is likely to violate the law. When a suspect site is identified, the page is downloaded and saved as potential evidence, and the operator of the site is sent an e-mail warning that explains the law and provides a link to educational information available at www.ftc.gov. Shortly thereafter, a law enforcement

cases involved show the extent to which alleged online crime . . . involves the blending of traditional crimes with various forms of computer crime." *Id.*

170. *Id.*

171. *Id.*

172. *Id.*

173. *Id.* ("To conceal his activities, he hired secretaries in five states outside Utah to receive payments from would-be buyers, used an e-mail service based in Australia, and used an anonymizing program when conducting online activities.").

174. *Id.*

175. *Internet Fraud Hearing*, *supra* note 58, at 20 ("The [Federal Trade] Commission's efforts to improve consumer complaint collection and analysis through the Consumer Response Center and Consumer Sentinel [Database] are complemented by a proactive program to uncover fraud and deception in broad sectors of the online marketplace through 'Surf Days.'"). As of the time of this hearing, in May of 2001, the FTC had conducted twenty-seven separate Surf Days. *Id.* at 24.

176. *Id.* at 24.

> team revisits the previously warned sites to determine whether they have remedied their questionable claims or solicitations.[177]

The targets of Surf Days range from "'cure-all' health claims to fraudulent business opportunities and credit repair scams."[178] Although the Surf Day concept seems basic, it has been effective in helping to rid the Internet of shady operations. Between 20% and 70% of people who receive warnings from the FTC as a result of Surf Days promptly comply with the applicable law.[179] Surf Days have been so effective that they are now widely used by various government agencies, consumer groups, and other private organizations.[180]

3. EDUCATIONAL MEASURES

Perhaps the most effective way to combat Internet fraud against the elderly is to stop it before it starts. An effective preemptive strategy includes a proactive educational regime. The FTC plays a prominent role in educating the public about consumer fraud and "has developed a rich collection of data that enable [it] to detect activities that cause significant consumer harm."[181] In particular, the FTC maintains the Sentinel database to track and prevent Internet fraud by disseminating information to the public through a network of government agencies.[182] The Sentinel database stores information regarding fraud complaints submitted by consumers as well as various external government agencies and contributors.[183] The FTC distributes the fraud complaints stored on the Sentinel database to more than 1300 law enforcement agencies, effectively setting up an information network with direct access to all participating agencies.[184] The agencies can then notify members of the general public as they see fit, often in the

177. *Id.* at 23.
178. *Id.* at 24.
179. *Id.* at 23.
180. *Id.* at 24 ("More than 250 law enforcement agencies or consumer organizations around the world have joined the Commission in these activities; collectively, they have identified over 6,000 Internet sites making dubious claims.").
181. *New Victims*, *supra* note 31, at 8 (prepared statement of the FTC).
182. *Id.*
183. *Id.* (explaining that these external contributors include the FBI's Internet Crime Complaint Center, Canada's Phonebusters, local chapters of the Better Business Bureau, the U.S. Postal Inspection Service, and the Social Security Administration's Office of Inspector General). Further, Sentinel "provides access to other investigative tools, including a library of telemarketing tapes, points of contact in domestic and foreign agencies, and model forms and pleadings for both criminal and civil fraud prosecutions." *Id.* at 8 n.3.
184. *Id.*

form of press releases, Web sites, and word of mouth.[185] However, because the FTC and its network are not solely concerned with the elderly demographic and its susceptibility to Internet fraud, it may be difficult for elderly people to efficiently retrieve the specialized information they need to protect themselves.[186]

In some states, various entities have created specialized groups whose mission is to serve, protect, and educate the elderly. For example, the Coalition of Wisconsin Aging Groups (CWAG) Elder Law Center is dedicated to protecting the elderly from financial abuse by "educating and empowering the elderly to recognize, report, and combat scams and other fraudulent practices[, thus] minimiz[ing] the victimization of seniors and protect[ing] the viability of federal and state benefit programs."[187] The CWAG Elder Law Center utilizes a four-fold approach to protecting the elderly population from fraud: educating consumers, providing legal services to victims, encouraging investigation of elderly fraud, and advocating for increased funding and enhanced legislation.[188] Most notably, the CWAG Elder Law Center provides substantial educational outreach programs. It distributes informative booklets with such titles as "Elder Exploitation Basics," "Prevent and Protect," and "Identity Theft Toolkit" that "inform and instruct readers on ways to protect seniors from financial exploitation through properly executed directives, well-secured personal information, and informed financial decision-making."[189] Additionally, the group provides one-on-one counseling to help victimized elderly people develop a course of action to rectify their situation.[190]

In Portland, Oregon, a volunteer group called Elders in Action assists older adults with Internet fraud and other important issues.[191]

185. *Id.*

186. *See generally id.* at 62–68 (statement of Denise Park, Cognitive Neuroscientist and Professor, Beckman Institute, University of Illinois at Urbana-Champaign).

187. *Id.* at 75 (statement of Helen Marks Dicks, Director at the Elder Law Center of the Coalition of Wisconsin Aging Groups). "The Coalition of Wisconsin Aging Groups (CWAG) is a statewide federation of individuals and member groups that represents over 125,000 people. As a nonprofit, nonpartisan organization, CWAG pursues justice and quality of life for people of all ages through legal and legislative advocacy, education, and leadership development." *Id.* at 75 n.1.

188. *Id.* at 76.

189. *Id.* Other informative titles include "It Pays to Plan Ahead" and "Plan." *Id.*

190. *Id.* at 77.

191. *New Victims*, *supra* note 31, at 81 (statement of Vicki Hersen, Director of Operations for Elders in Action). The mission of Elders in Action is "[t]o assure a vibrant community through the active involvement of older adults." Elders in Ac-

Elders in Action disseminates information to the public via its newsletters, brochures, electronic news line, and Web site, while its volunteers "provide personal support, information, guidance, and advocacy to fill gaps in meeting the needs and solving the problems for [the] growing senior population."[192] With an innovative philosophy embodying the concept "neighbor helping neighbor," Elders in Action advocates that the way to break the cycle of victimization that takes place on the Internet is through open communication and preventing senior isolation.[193] Specifically, Elders in Action actively encourages seniors to call its office if they receive a suspicious e-mail or are unsure as to the legitimacy of an e-mail.[194] Elders in Action also assists the elderly in recovering assets that have been lost to fraudulent schemes.[195]

Another method of educating the elderly with respect to Internet fraud is to provide classroom training. In Waterloo, Iowa, Hawkeye Community College runs a Senior Tech Program that offers a variety of classes "for people 50 and older with little or no computer experience."[196] For example, one class teaches students how to use the Internet and e-mail.[197] According to Tom Tierney, one of the program's instructors, most students in the class are in their sixties to early seventies.[198] Program Director Mike Tompkins reports a strong demand for the program in Iowa.[199] However, he is not aware of many other community colleges in Iowa that offer a program similar to the Senior Tech Program.[200] Ann Black, an employee at the Iowa office of the AARP, reports that the demand for classes like those offered by the Senior Tech Program now outpaces the training opportu-

tion, http://www.eldersaction.org/ (last visited Aug. 18, 2006). The organization represents the interests of seniors in the Portland metropolitan area through volunteer-driven programs. *Id.*

192. *Id.*

193. *Id.*

194. *Id.*

195. *Id.*

196. Wind, *supra* note 19. As of February 2006, more than 425 people have gone through the Senior Tech Program. *Id.*

197. *Id.*

198. *Id.* However, the Senior Tech Program frequently has students in their upper seventies and lower eighties. *Id.* One current student, Walter Boeke, is ninety-one years old and is learning how to use the Internet and how to send and receive e-mail. *Id.*

199. *Id.*

200. *Id.* ("[Tompkins] said a class has started in Sioux City [Iowa] since HCC's program began[, but he is not aware of any other such classes].").

nities that are available to the elderly in the state of Iowa.[201] Although seniors possess the desire, patience, and will power to become acquainted with new technology, the outlets for doing so are severely limited.[202] Educational opportunities like the Senior Tech Program are exactly what many elderly people need to build confidence and learn how to protect themselves as they venture into cyberspace.

One of the most creative programs aimed at educating the elderly for their voyage into cyberspace takes place overseas. In the United Kingdom, telecom giant British Telecommunications Plc (BT) held "Grandparents Day" on September 24, 2005.[203] As part of BT's Grandparent's Day, the corporation urged young people to become "Internet rangers" and educate the elderly generation on how to effectively and safely use the Internet.[204] The corporation believes that younger generations are in the best position to educate the elderly about computers and Internet technology.[205] The philosophy behind Grandparent's Day is that a true mutually beneficial relationship forms between the young and the elderly when the young take it upon themselves to teach the elderly the ways of the Internet. "'It's a real morale boost for young people as they assume the role of teacher and mentor, and to the older generation[,] the [I]nternet can open up a whole new world where hobbies and interests can be explored.'"[206] Although BT's program is primarily concerned with closing the digital divide, programs like this can easily be used as vehicles to educate the elderly with respect to Internet fraud.[207] To be effective, an educational regime must specifically target the elderly, be widely accessible, and present information in an inventive, clear, and understandable manner.[208] Programs like BT's Grandparent's Day are exactly the type

201. *See id.*

202. *See generally id.* (stating that there are not enough computer education classes to serve the older and retired adults in Iowa who want to become computer literate).

203. *Kids to Teach Elderly Net Skills*, BBC NEWS (U.K.), Sept. 24, 2005, http://news.bbc.co.uk/1/hi/technology/4276068.stm.

204. *Id.*

205. *Id.* ("'With the [I]nternet becoming the communication tool of choice for fundamental services like medical information and education, the digitally excluded will be significantly disadvantaged when trying to access services and information.'" (quoting Mike Hughes, Head of Digital Inclusion for BT)).

206. *Id.*

207. *See generally id.*

208. BT, for example, launched a special website with "tools, advice, and activities to assist children to help their grandparents get the most from the [I]nternet." *Id.*

of proactive and creative educational programs the United States must implement to reduce the incidence of Internet fraud against the elderly.

IV. Resolution

A. The Urgent Need for Action

To resolve the growing problem of the elderly falling victim to Internet fraud, it is clear that society must do at least one thing—act now. Although older Americans currently comprise a relatively small minority of the Internet population, this will not be the case for much longer, as members of the sixty-five and older population are introducing themselves to the Internet with increasing frequency. If society remains complacent and continues to ignore the growing elderly population on the Internet, the elderly will invariably continue to be victimized.

B. Legislation and Prosecution Alone Will Not Remedy the Problem

Although legislation specifically tailored to address Internet fraud serves necessary deterrent and retributive purposes, it does not adequately address the unique nature of the problem at hand. The convoluted legislative process is too slow to keep up with the Internet and the unique challenges it presents. Internet technology will always stay at least a few steps ahead of the law. For example, although the federal government recognized in the summer of 2003 that phishing was "the hottest, and most troubling, new scam on the Internet,"[209] Congress has yet to pass the APA.[210] Although the elderly are in urgent need of protection, the APA continues to sit dormant in Congress. Even if the APA is successfully drafted into law, legislation that addresses Internet fraud has severe practical limitations, including the difficulties of finding the perpetrators of Internet-based crimes, obtaining personal jurisdiction over them, and enforcing any resulting penalties or judgments.

209. *Internet Fraud Hits Seniors*, *supra* note 13, at 78 (statement of David Jevans, Chairman, Anti-Phishing Working Group).

210. THOMAS, S. 472, *supra* note 142.

Further, the aggressive prosecution of criminals who defraud the elderly does not constitute a comprehensive solution to the problem. Once an elderly person has been victimized, the damage from the fraud has already been done. Post-victimization prosecutorial measures are inadequate as they often provide elderly victims with little redress. The elderly psyche is typically fragile, and it is common for elderly people to suffer irreversible emotional harm once they are victimized.[211] The prosecution of a criminal serves as little comfort to an elderly victim who has had his or her life savings and hard-earned assets stolen. Moreover, time is a scarce resource among the elderly. Many elderly people do not have the time or the desire to spend their latter years partaking in legal proceedings and attempting to reacquire misappropriated assets. Consequently, society must not merely rely on legislative and prosecutorial measures to sufficiently protect the elderly.

C. Preemptive Measures

The war against Internet fraud must be waged on multiple fronts, and the key component to protecting the elderly is preemptive education. However, not just any educational regime will suffice. Teaching the elderly to safely use the Internet and to avoid victimization requires an educational approach that is creative, proactive, and highly accessible.

The responsibility of educating the elderly must fall squarely on the shoulders of those who already posses knowledge of the Internet. A large portion of this burden should fall on today's youth, but family, friends, neighbors, and local organizations must also contribute. We as a society must embrace the "neighbor helping neighbor" philosophy of Elders in Action.[212] There exists a vast knowledge disparity between the elderly and younger generations with regard to the Internet. Most elderly regard as incomprehensible what many seasoned Internet users regard as second nature. Thus, even small amounts of time spent educating the elderly will pay huge dividends and help close the knowledge gap.

211. Press Release, U.N. Dep't of Pub. Info., Elder Abuse Widespread and Unreported, Says New Report by Secretary-General, U.N. Doc. DPI/2264 (Mar. 2002), *available at* http://www.un.org/ageing/prkit/elderabuse.htm.

212. Elders in Action, *supra* note 191.

Members of younger generations should take responsibility for initiating progressive educational programs like BT's Grandparent's Day[213] in the United States. A program whose premise is the young helping the old is mutually beneficial. While the elderly learn from younger generations about technology and the Internet, the young benefit from exposure to the life experiences and wisdom of the elderly. Additionally, local communities must pool together resources and offer classes designed to teach older Americans to efficiently and safely use the Internet. The success of the Senior Tech Program in Waterloo, Iowa[214] demonstrates that the elderly demand for computer and Internet training is real. Elderly demand is, in fact, so high that it greatly exceeds the supply of such training. Community colleges, high schools, local businesses, and others should all pitch in and attempt to meet this demand.

V. Conclusion

The Internet is no longer limited to the young and tech-savvy. Incredible advances in technology have made today's Internet available to all demographics—the elderly included. However, this creates problems. As the elderly migrate to the Internet, fraudulent schemes targeting them follow. As with traditional forms of fraud, the elderly are particularly vulnerable to these schemes perpetrated over the Internet. Action must be taken now, before this problem gets worse. To adequately protect the elderly, a war against Internet fraud must be waged on multiple fronts. However, the most vital component of this war is education. Educational programs that are creative and specifically tailored to reach the elderly are the key to reducing the number of elderly Internet fraud victims.

213. *Kids to Teach Elderly Net Skills*, *supra* note 203.
214. Wind, *supra* note 19.