1-1-2002

Oh No, Grandma Has a Computer: How Internet Fraud Will Take the Place of Telemarketing Fraud Targeting the Elderly

Leda Mouallem

Follow this and additional works at: http://digitalcommons.law.scu.edu/lawreview

Part of the Law Commons

Recommended Citation
Leda Mouallem, Comment, 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 (2002).
Available at: http://digitalcommons.law.scu.edu/lawreview/vol42/iss2/7

This Comment is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara Law Review by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
OH NO, GRANDMA HAS A COMPUTER: HOW
INTERNET FRAUD WILL TAKE THE PLACE OF
TELEMARKETING FRAUD TARGETING THE
ELDERLY

Leda Mouallem*

I. INTRODUCTION

"Most Internet fraud has clear antecedents in telemarketing fraud. [The difference] is the size of the potential market, and the relative ease, low cost, and speed with which the scam can be perpetrated." The elderly have long been targets and victims of consumer fraud. Since the most popular medium among fraud perpetrators is the telephone, government and law enforcement agencies have been battling telemarketing fraud for years.

This comment will evaluate the fraud that is being perpetrated against the elderly today, specifically commenting on the newest guise threatening elderly persons: Internet consumer fraud. First, the traditional telemarketing fraud industry, and current regulatory schemes, will be surveyed.

* Comments Editor, Santa Clara Law Review, Volume 42. J.D. candidate, Santa Clara University School of Law; B.A., University of California, Davis.
2. See generally Jeffrey L. Bratkiewicz, "Here's a Quarter, Call Someone Who Cares"; Who is Answering the Elderly's Call for Protection from Telemarketing Fraud, 45 S.D. L. REV. 586 (2000).
3. See Fraud Against Seniors, supra note 1.
4. See infra Part II.A.
Second, this comment will evaluate modern day advances in technology that allow telemarketers to operate in a new medium, as well as current legislation that attempts to address this problem. Finally, this comment will present possible solutions to the problem, such as amending current legislation, educating the elderly population about the prevalence of fraud on the Internet, and arming the elderly with certain advanced technology in order to curtail the potentially limitless abuse of the elderly by perpetrators of Internet fraud.

II. BACKGROUND

A. Telemarketing Fraud Against the Elderly

For at least the last fifteen years, con-artists have utilized telemarketing schemes as a means to perpetrate fraud upon unsuspecting consumers. Consumer losses incurred from telemarketing fraud range from at least $3 billion to as much as $40 billion dollars annually.

AARP (formerly known as the American Association of Retired Persons) estimates that nearly ten percent of all telemarketing firms participate in fraudulent and deceptive practices. Furthermore, these estimates only take into account fraudulent telemarketing practices in the United States; they do not account for fraudulent activity in countries that base their operations outside of the United States in order to avoid state and federal penalties.

5. See infra Part II.B.
6. See infra Part IV.
7. See infra Part V.
9. See Fraud Against Seniors, supra note 1.
10. AARP is an organization that caters to informing and educating the midlife and elderly generations on a variety of issues that affect middle aged and elderly persons. For more information on AARP, visit the organization's Web site at http://www.AARP.org/.
11. See Bratkiewicz, supra note 2, at 587.
12. See id.
INTERNET FRAUD

Although consumers of all ages fall prey to fraudulent telemarketers, senior citizens are disproportionately affected. AARP reports that fifty-six percent of the victims of telemarketing fraud are age fifty or older, and in certain telemarketing scams eighty percent of the victims are age sixty-five or older. AARP estimates that Americans over the age of fifty lose approximately $14.8 billion dollars every year to telemarketing scams. A review of the reasons telemarketers target the elderly makes it easier to understand these figures.

1. The Elderly Population in the United States is Booming

The elderly represent the fastest growing population group in the United States. There are currently thirty-five million persons age sixty-five and older, representing approximately 12.4% of the total population. This number is expected to increase to seventy million, or roughly twenty percent of the entire U.S. population, by the year 2030. The boom in the elderly population may be due to increased life expectancy, which is currently seventy-nine years for women and seventy-four years for men. Therefore, fraudulent telemarketers have a vast resource of persons to target in the expanding elderly population.

2. Additional Reasons for Targeting the Elderly

There are numerous reasons that telemarketers are

13. See id. at 588.
15. See Fraud Against Seniors, supra note 1.
16. See Bratkiewicz, supra note 2, at 587.
17. See id. at 588-89.
18. See id. at 586.
thought to prey upon the elderly including (a) their lack of mobility, (b) their frailty, and (c) their financial resources.  

a. Lack of Mobility

Older Americans are often retired from full-time work. Many spend the vast majority of their time at home, and therefore provide an easy target for telemarketers looking for prey. Additionally, seniors often suffer from physical illness and greater functional disability, requiring them to stay close to or remain in their homes for long periods of time. For these reasons, seniors are more likely to be home to answer the phone when telemarketers call.

b. Frailty

In addition to preying on the elderly because telemarketers know they will be available to answer phone calls, telemarketers also rely on the fact that seniors are more likely to remain on the phone to hear what they have to say. Telemarketers construct their scams to offer products and opportunities that will interest the elderly, such as health care needs, investment and business opportunities, prize promotions, lottery clubs, charitable causes and travel packages. Telemarketers take into consideration the fact that elderly persons are more likely than other age groups to have feelings of isolation and depression, combined with deteriorating physical and mental capabilities. It is estimated that

22. See Bratkiewicz, supra note 2, at 588; 145 CONG. REC. S3499 (1999) (statement of Sen. Tom Daschle (D-S.D.)) (commenting on the Seniors Safety Act of 1999) (stating that “[s]eniors are often targeted by criminals because of their lack of mobility, isolation, and dependence on others”).
23. See AARP & HHS, supra note 20, at 11-12.
24. See Bratkiewicz, supra note 2, at 589.
25. See AARP & HHS, supra note 20, at 12-14.
26. A survey conducted by AARP “shows that elderly consumers find it difficult to terminate telephone conversations, even when they say they are not interested in continuing a conversation.” See Fraud Against Seniors, supra note 1; see also Bratkiewicz, supra note 2, at 589; Marlys J. Harris, Elder Fraud, MONEY, Nov. 1, 1995, at 149 (suggesting that elderly persons may not hang up on telemarketers because seniors are often too courteous or genuinely appreciate the company).
27. See Bratkiewicz, supra note 2, at 591; see also Fraud Against Seniors, supra note 1.
28. See U.S. DEP'T OF JUSTICE, HEARING BEFORE THE UNITED STATES SENATE SPECIAL COMMITTEE ON AGING (1996), at
15.4% of persons age sixty-five to sixty-nine, 20.5% of persons age eighty to eighty-four, and 22.6% of persons age eighty-five and older suffer from severe symptoms of depression, suggesting that depression increases with age. Depression is closely associated with higher rates of physical illness, greater functional disability, and higher health care resource utilization. The elderly generation faces these realities daily. It is also theorized that since elderly persons suffer from feelings of isolation and loneliness, they crave human contact and friendship, which makes it easier for fraudulent telemarketers to victimize elderly persons.

AARP disputes the theory that elderly persons are victimized because of their frailty. Research conducted by AARP suggests that only twenty-eight percent of elderly telemarketing fraud victims actually live alone. Furthermore, AARP contends that eighty percent of telemarketing fraud victims have family living nearby. The research also indicates that most elderly telemarketing fraud victims are well-educated, affluent, and socially active. Despite disagreement regarding the precise reason elderly persons are targeted by fraudulent telemarketers, the fact remains that the elderly are disproportionately affected.

c. Financial Resources

Fraudulent telemarketers often target the elderly because they have financial resources readily available. Unlike younger generations, most elderly persons no longer have financial obligations, such as mortgages, car payments, and

---


29. See FEDERAL INTERAGENCY FORUM ON AGING-RELATED STATISTICS, supra note 21, at 76 tbl.16.
30. See id.
31. See Bratkiewicz, supra note 2, at 589.
32. Id. at 590.
34. See id.
35. See id.
36. See Fraud Against Seniors, supra note 1.
37. See id.
their children's educational expenses. Fraudulent telemarketers take advantage of the fact that many older people have cash reserves and other assets to spend on seemingly attractive offers. The income of the elderly is mainly derived from social security, pension benefits, and income from assets and continued earnings. The median net worth of persons age sixty-five or older has steadily increased over the last several years. Although there is general agreement that net worth among all households has increased over time, data sources disagree about the amount of this increase. The bottom line, however, is that the financial situation of the elderly makes them incredibly attractive targets for perpetrators of telemarketing fraud.

3. Types of Telemarketing Fraud Most Commonly Perpetrated Against the Elderly

Several telemarketing scams specifically target the elderly, and these scams are only limited by the creativity of the criminally-deviant mind. The most common types of telemarketing schemes include: (a) deceptive prize promotions and lottery clubs, (b) telefunders or bogus charities, (c) investment and business opportunity scams, (d) recovery scams, and (e) credit card loss protection scams.

a. Deceptive Prize Promotions/Lottery Clubs

The deceptive prize promotions/lottery club scam is one of the top five scams most often reported to the Federal Trade Commission ("FTC"). In this scam, the elderly consumer receives a call congratulating him or her on having been selected to win cash, a car, vacation or jewelry. The consumer is then required to send payment, usually by an overnight courier service, in order to receive the prize. After the elderly consumer sends the money, the prize is never received, or

38. See id.
39. See AARP & HHS, supra note 20, at 10.
40. See id. at 9. Net worth is defined as the value of real estate, stocks, bonds and other assets minus outstanding debts.
41. See Bratkiewicz, supra note 2, at 590.
42. See Fraud Against Seniors, supra note 1.
43. See id.
44. See id.
45. See id.
it is an item of little value.\textsuperscript{46} Losses per consumer for telemarketing prize promotions can range from a few hundred to thousands of dollars.\textsuperscript{47} In the most severe circumstances, elderly consumers have lost their entire life savings.\textsuperscript{48} Due to the popularity of this scam amongst fraudulent telemarketers and the devastating impact it can have on elderly victims, the FTC frequently targets fraudulent prize promotion type scams.\textsuperscript{49} The FTC conducted eighty enforcement actions against 119 defendants in twenty-six states in the years 1996-2000.\textsuperscript{50}

b. Telefunder or Bogus Charities

Another common type of telemarketing fraud often aimed at elderly persons involves telephoning consumers and either enticing them to donate money to bogus charities, or in some other way misrepresenting the way a donor’s money will be used.\textsuperscript{51} Efforts to combat this type of fraud by the FTC have resulted in ten federal enforcement actions and eighty-six state enforcement actions.\textsuperscript{52} Additionally, AARP has taken steps to warn elderly consumers about deceptive charitable fundraisers by setting up phone centers that provide consumers with information about legitimate charities.\textsuperscript{53}

c. Investment and Business Opportunity Fraud

Elderly persons are often susceptible to scams that involve new business opportunities,\textsuperscript{54} or investment scams that offer high rates of return.\textsuperscript{55} These types of offers are highly attractive to older persons who have recently retired\textsuperscript{56} or are seeking financial security and autonomy.\textsuperscript{57} Business oppor-

\textsuperscript{46} See id.
\textsuperscript{47} See id.
\textsuperscript{48} See Fraud Against Seniors, supra note 1.
\textsuperscript{49} See id.
\textsuperscript{50} See id.
\textsuperscript{51} See id. In a study done by the FTC in 1994 on five illegal telefunding operations, eighty-five percent of the consumers were sixty-five years of age or older. See id.
\textsuperscript{52} See id.
\textsuperscript{53} See id.
\textsuperscript{54} See Fraud Against Seniors, supra note 1.
\textsuperscript{55} See Bratkiewicz, supra note 2, at 589-91.
\textsuperscript{56} See Fraud Against Seniors, supra note 1.
\textsuperscript{57} See Bratkiewicz, supra note 2, at 593.
tunity scams involve the con-artist calling the consumer and offering him an opportunity to operate a small business or to work from home. The telemarketer touts that with little work or cash outlay, the consumer will reap incredible profits, citing such figures as $1000 dollars a day or more.

To make the business venture sound legitimate, the telemarketer provides the consumer with the names and telephone numbers of other consumers who have successfully taken advantage of the business opportunity. In actuality, these individuals are also involved in the scam, and they lie to the consumer about the reality of the business venture. Consumers in these type of scams lose anywhere from hundreds to tens of thousands of dollars.

Similarly, investment opportunity scams promise outrageously high profits for little or no effort on the part of the consumer. In these scams, the investor is promised extremely high rates of return with no risk. There are several different types of investment schemes, including the “Pump and Dump,” the “Pyramid,” the “Risk-free” fraud, and “Off-shore” frauds.

60. See Fraud Against Seniors, supra note 1.
61. See id.
62. See id.
63. See id.
64. See id.
65. This version of investment fraud involves the perpetrator hyping a particular company and its stock in order for investors to purchase stock. See John Rothchild, Protecting the Digital Consumer: The Limits of Cyberspace Utopianism, 74 IND. L.J. 893, 906-07 (1999). Once the stock has been purchased, the perpetrators will stop hyping the stock to other consumers and the price of the stock will fall. See id. Small, thinly traded companies are most often used because there is little or no information available about the company. See id.
66. The Pyramid or “Ponzi” scam is a very popular type of investment scam where the fraudulent participants tout that an investor can turn a certain amount of money into a greater amount. See id. at 905-06. The “profit” that is to be given to the consumer comes from the investment of other consumers. See id. The participants make money by recruiting new consumers until, at some point, the money runs out and the consumer has lost his investment. See id.
67. In this classic type of investment fraud, the investor is promised incredible returns for little or no risk. Often times the companies and products being offered do not even exist.
68. Off-shore investment scams consist of inviting an investor to invest in
The FTC and the U.S. Department of Justice ("DOJ") have led several concerted efforts in cooperation with state law enforcement agencies to stop these types of scams. Nearly one hundred actions have been brought against operators of fraudulent business opportunity schemes.

d. Recovery Scams

Recovery scams often target the elderly and involve the re-victimization of consumers who fell prey to an earlier scam. In this scam, the fraudulent telemarketer calls the elderly victim and offers to recover money lost through a previous scam in exchange for a small fee. Quite often, the same individuals who defrauded the consumer the first time execute the second scam. The money is never recovered and the elderly person is thus victimized twice and robbed of an additional sum of money. Losses per elderly consumer from this type of scam range from a few hundred dollars to thousands of dollars. Today, these types of scams have almost vanished due to aggressive enforcement by the FTC and DOJ, as well as strict federal regulations.

69. The U.S. Department of Justice ("DOJ") is a government agency that works with another government agency, the FBI's Criminal Fraud Division, to enforce the criminal statutory provisions that govern telemarketing activities. The DOJ also has authority to enforce civil statutory provisions as well. For additional information regarding the DOJ's efforts to eradicate telemarketing fraud, see U.S. DEP'T OF JUSTICE, WHAT'S THE DEPARTMENT OF JUSTICE DOING ABOUT TELEMARKETING FRAUD?, at http://www.usdoj.gov/criminal/fraud/telemarketing/doi.htm (last updated Sept. 25, 1998).

70. These agencies work together in concerted undercover operations that target certain types of telemarketing fraud at any given time. These operations are referred to as "sweeps." See Fraud Against Seniors, supra note 1.

71. See id.

72. See id. One survey taken by the FTC in a specific recovery room case found that eighty-one percent of the victims were at least sixty-five years of age, forty-seven percent were at least seventy-five years of age, and twenty-three percent were at least eighty years of age. See id. Similar statistics have been found in similar cases. See id.

73. See id.

74. See id.; Bratkiewicz, supra note 2, at 592 (explaining the way a recovery scam works).

75. See Fraud Against Seniors, supra note 1.

76. See id.

77. See discussion infra Part II.A.4.
e. Credit Card Loss Protection

The final type of scam most often perpetrated by fraudulent telemarketers involves convincing consumers to buy worthless credit card loss protection and insurance programs. This type of fraud also disproportionately affects seniors. Here, the telemarketer poses as a representative from the credit card's security department and scares the consumer with false stories regarding credit card liability for unauthorized charges. The telemarketer then suggests that the consumer purchase protection in order to avoid liability for any unauthorized charges. The consumer purchases the fraudulent credit card protection and the payment is then kept by the telemarketer. The FTC has also made attempts to combat this type of fraud and, to date, has brought four federal actions and seven state actions against these types of fraudulent operations.

4. Regulatory Agencies and Legislative Impact

In order to address the problem of telemarketing fraud, Congress has proposed and enacted legislation, and the FTC and DOJ have undertaken active enforcement of these statutes. Under sections 5 and 13(b) of the Federal Trade Commission Act, the FTC has the authority to file civil actions, seek immediate injunctive relief against fraudulent telemarketers and obtain restitution for injured consumers. If restitution is impossible, the FTC can seek disgorgement of the fraudulently collected monies. In the past three years, the FTC has collected over sixty-one million dollars in judgments for consumer redress or disgorgement to the Treas-

78. See Fraud Against Seniors, supra note 1.
79. See id. In a recent study on telemarketing fraud, the National Consumer's League reported that seventy-one percent of the credit card loss protection plan complaints received by the National Fraud Information Center were made by consumers age fifty or older. Id.
80. See id.
81. See id.
82. See id.
83. See id.
84. See Fraud Against Seniors, supra note 1.
86. See Fraud Against Seniors, supra note 1. Injunctive relief will immediately halt all illegal activity. See id.
87. See id.
The DOJ, through the FBI's Criminal Fraud Division, enforces the criminal statutory provisions that govern telemarketing activities. The DOJ is also authorized to seek civil injunctions and related relief. The legislation governing telemarketing fraud and authorizing the law enforcement actions discussed above are discussed in turn below.

a. Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994 and the Telemarketing Sales Rule

Congress passed the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act") in 1994, which granted the FTC broad authority to regulate telemarketing fraud. The Telemarketing Act provides for a joint state/federal enforcement plan, which allows state Attorneys General to bring suit in federal court for violations of the Telemarketing Act. In an effort to punish telemarketing criminals in a more comprehensive manner, this act allows criminals to be prosecuted by both state and federal officials.

Following Congress's lead, in 1995, the FTC enacted the Telemarketing Sales Rule ("Sales Rule"), which specifically defines and prohibits deceptive telemarketing practices. The Sales Rule protects consumers by prohibiting telemarketers from calling any consumer who has previously requested not to be contacted by the particular telemarketer. It also prohibits telemarketers from calling consumers before 8:00 a.m. or after 9:00 p.m. in the consumer's local time zone.

Both the Telemarketing Act and the Sales Rule have greatly enhanced the FTC and the DOJ's regulation and en-

88. See id.
89. See U.S. DEPT OF JUSTICE, supra note 69.
90. See id.
92. See id.; see also Fraud Against Seniors, supra note 1.
94. See id. §§ 6102-6105, 6107.
95. See 16 C.F.R. §§ 310.1-310.8 (2001); see also Fraud Against Seniors, supra note 1.
96. See 16 C.F.R. §§ 310.1-310.8; see also Proposed Legislation, supra note 8.
97. See 16 C.F.R. § 310.4(c).
forcement powers to stop fraudulent telemarketers. The effectiveness of the Telemarketing Act and the Sales Rule will be analyzed in a report to Congress that should be made in the near future. The Telemarketing Act requires the FTC to perform this evaluation five years after the adoption of the Sales Rule. Based on the information received during this review, the FTC will determine whether the Telemarketing Act needs to be modified, and will report its findings to Congress.

b. Senior Citizens Against Marketing Scams Act of 1994

The Senior Citizens Against Marketing Scams Act of 1994 ("SCAMS"), which was enacted by Congress specifically for the purpose of protecting the elderly from marketing fraud, added to the regulatory powers already provided for in the Telemarketing Act. SCAMS provides increased penalties for telemarketing fraud that victimizes the elderly by allowing federal courts to add up to five additional years for any offense connected to telemarketing activities, and up to ten additional years if the offense either targeted persons older than fifty-five years, or victimized ten or more persons age fifty-five or older.

c. Seniors Safety Act of 1999

The Seniors Safety Act of 1999 ("SSA") was proposed by Senators Patrick Leahy (D-Vt.), Tom Daschle (D-S.D.), Edward Kennedy (D-Mass.), and Robert Toricelli (D-N.J.) for the purpose of enhancing the Telemarketing Act. A major goal of the SSA is to "increase protections for victims of telemar-

98. See Bratkiewicz, supra note 2, at 594.
99. See id. at 595.
100. See id. The evaluation was to take place in 2000. As of the date of the writing of this comment, the evaluation has not yet been conducted or reported.
101. See Proposed Legislation, supra note 8.
103. See Bratkiewicz, supra note 2, at 595.
104. See 18 U.S.C. § 2326. The criminal offenses that are currently enforced by the DOJ include wire fraud, mail fraud, and conspiracy to engage in wire and mail fraud. See id. Each of these offenses carries a maximum term of five years. See id. SCAMS adds five to ten years to these penalties. See id.
keting fraud . . . " The SSA gives the Attorney General the authority to block or terminate telephone service to facilities that are being used to conduct fraudulent activities. Another feature of the SSA is the establishment of a "Better Business Bureau" type center that provides seniors and their families access to information about the legitimacy of telemarketing operations. A unique aspect of the SSA is that it addresses Internet fraud perpetrated against the elderly. The SSA is currently pending in the Senate.

B. Use of Computers and the Internet by the Elderly

Not only are the elderly a growing population group in the United States, but they are increasingly likely to use the Internet, i.e., to get "wired." There are at least 7.5 million Internet users over the age of fifty, and this number is projected to increase. The number of elderly persons who accessed the Internet in 1999 increased in the year 2000, and increased again in the year 2001.

There are several possible reasons for this increase. Both innovative and traditional goods can be purchased faster and at lower prices through the Internet. Additionally, access to

107. Id. at S3490.
108. See id.
110. See S. 751 § 301(a).
111. The SSA also expands the scope of the SCAMS Act by replacing “telephone calls” in 18 U.S.C. § 2325(1) with “wire communications utilizing a telephone service,” presumably to include Internet transmission conducted via telephone wire. See S. 751 § 302(a); Bratkiewicz, supra note 2, at 596. Criminal penalty enhancements are also contained in the SSA. See S. 751 § 302(b).
112. The last major action concerning this legislation took place on March 25, 1999, when it was referred to the Senate committee. See also 146 CONG. REC. S11, 366-67 (statement of Sen. Leahy) (requesting consideration for the SSA).
113. See HETZEL & SMITH, supra note 19, at 1-3.
116. See id.
117. See Fraud Against Seniors, supra note 1.
the Internet may provide the elderly with more independence, freedom and ease of living in their later years. People have access to items such as medical products and travel packages, and they can conduct various financial transactions on the Internet. The Internet also provides opportunities for isolated elderly persons to establish communications and friendships through chat rooms, bulletin boards and electronic mail ("email"). There are several Web sites that cater especially to elderly persons, offering health care information, guides to using computers and the Internet, links to the personal homepages of other elderly persons, and email pen pal services.

Despite the benefits the Internet offers to the elderly, it also creates the potential for widespread fraud and deception. The same con-artists who once used the telephone as their means to perpetrate fraud on the elderly can now target them through the Internet. Experts predict that online fraud will pose an even greater threat than telemarketing scams. Already nearly half of all Americans use the Internet, and there are 338 million Internet users globally. Furthermore, it is likely that the number of Internet users will continue to grow, both in the United States and around the world. Not only is it incredibly easy to access millions of people via the Internet,

118. A large number of different commercially-sponsored Web sites offer such services. Two examples can be found at the Web site addresses of http://www.excite.com and http://www.yahoo.com.

119. A chat room is a method by which Internet users can "talk" to each other when they are online by typing messages that other users can read and respond to. Bulletin boards are online meeting and announcement centers where participants can post and read messages, as well as carry on discussions. Electronic mail is an extremely popular way to communicate with other individuals quickly. Messages are sent from one person's computer to another's, usually in a much shorter time period than it would take for a letter to travel between the two people through the U.S. postal system.

120. Sponsors of such Web sites include Senior.com (http://www.senior.com), Senior-site.com (http://seniors-site.com/), SeniorNet (http://www.seniornet.org), SeniorGlobe.com (http://www.seniorglobe.com), and the U.S. Government through its "FirstGov for Seniors" site (http://www.seniors.gov/index.htm).


122. See id.

it is also inexpensive to conduct a scam on the Internet. Using a computer and modem, a con-artist can erect and maintain a Web site for a minimal amount of money. Comounding this problem is the advent of new technologies, which make it easier for con-artists to maintain a fraudulent Internet operation.

1. Modern Day Alternatives to Analog Phone Lines

The traditional way to connect to the Internet is through the use of an analog modem, which is a device that converts data from a computer to a form that can be transmitted over telephone wires to another computer where a similar device reconverts it. In common parlance, when two modems establish a connection over telephone lines, they are “ready to talk.”

Studies show that this method of Internet access is rapidly declining and will be virtually eliminated by the year 2004, with only three percent of Internet users utilizing an analog modem. This is most likely due to the fact that even the fastest analog modems cannot compete with new technologies that allow users to connect to the Internet quickly without the use of “slow, noisy analog phone lines.”

Today, there are several technologies that make it possible to connect to the Internet without using a traditional analog phone line. Integrated Services Digital Network (“ISDN”) uses a special digital phone line. Digital Sub-

124. See Fraud Against Seniors, supra note 1. For a brief explanation of how a modem operates, see infra note 126 and accompanying text.
125. See discussion infra Parts II.B.1-4.
126. See MERRIAM-WEBSTER DICTIONARY 762 (9th ed. 1985). Since computer data are maintained in a digital form, but traditional telephone wires are capable of transmitting only analog signals, modems are necessary to convert signals from a digital form into analog, and vice versa. For greater detail regarding modems, and the forms of storing information, see NIELS JONKER, PRACTICAL GUIDE TO ANALOG MODEMS, at http://www.myhome.org/pg/modem.htm (visited Jan. 1, 2001).
128. See Mel Beckman, Modems Last Stand, MACWORLD, May 1999, at 86. See also Jones, supra note 127 (discussing why analog modems are no longer favorable due to their slow connection process to the Internet).
129. See Beckman, supra note 128, at 86.
130. See id.
scriber Line ("DSL") works by adding digital data transmissions to an ordinary analog phone line, thereby allowing both analog voice signals and digital data to be transmitted over the phone line.131

Consumers can also connect to the Internet using a satellite.132 Satellite Internet connections use an analog modem to send data out from a computer, and a satellite to receive data. The satellite then beams the information to your computer. This method of connection is reportedly eight to fourteen times faster than an analog modem alone, and four times faster than an ISDN line.133 It is expected that in the near future satellites will be used for both sending and receiving data, and that sending data through analog phone lines will be eliminated.

ISDN, DSL, and satellite-based connections are extremely popular alternatives to the traditional analog modem because they connect to the Internet much faster and with fewer problems than the analog system.134 Like the analog modem, ISDN, DSL, and satellite connections require a user to have service through a phone company.

2. Connecting to the Internet Without Using a Phone Line

Newer technologies, such as cable modems, allow users to connect to the Internet without use of a phone line.135 Furthermore, certain technologies eliminate even the need for a computer to connect to the Internet.136

Instead of using phone lines to transmit data, cable modems deliver high-speed data over cable television ("TV") lines.137 Although a cable connection to the Internet is much faster than analog modem connections and ISDN or DSL,138 a

131. See id.
134. See id.
135. See Gilroy & Kruger, supra note 132, at 2-4.
136. See discussion infra Part II.B.3.
137. See Beckman, supra note 128; Jones, supra note 127.
138. See Jones, supra note 127.
potential drawback is that the speed may vary due to the fact that one television cable must simultaneously service all users in the same area, and may easily get congested.\textsuperscript{139} In addition, cable modems are not available in all geographical areas, although cable modem Internet access is increasingly becoming available to more consumers.\textsuperscript{140} However, because of the extraordinary speed with which cable modems connect to the Internet, they are an increasingly popular choice among consumers.\textsuperscript{141} There are an estimated 2.3 million subscribers, and this number is expected to increase to 9.2 million by the year 2003.\textsuperscript{142}

3. \textit{Alternatives to Computers: Mobile Internet Devices and Wireless Connections}

In addition to the various alternative ways to connect to the Internet using a computer, today there are technologies that will allow devices, other than computers, to connect to the Internet. Such devices include mobile phones, pagers and Personal Digital Assistants ("PDAs"), which are smaller, mobile versions of a personal computer.\textsuperscript{143} In order to access the Internet through one of these devices, a new technology called Wireless Application Protocol ("WAP") is used.\textsuperscript{144} WAP delivers web-like content to mobile devices.\textsuperscript{145} Originating in Finland, where more than seventy percent of the population uses mobile phones, WAP allows users to browse sites on the Internet, retrieve information and enter data.\textsuperscript{146} At the moment, consumers who wish to use WAP technology to access the Internet through their mobile

\textsuperscript{139} See \textit{id.}.
\textsuperscript{140} See David Lake, \textit{Bandwidth Bandwagon}, \textit{THE INDUSTRY STANDARD} (May 15, 2000), at \url{http://www.thestandard.com/article/0,1902,15018,00.html}.
\textsuperscript{141} See \textit{id.}
\textsuperscript{142} See \textit{id.}
\textsuperscript{143} See Advertisement, Michael Mullen for ZDNet Reviews, CNET Networks, Inc., \textit{A Beginners Guide to PDA's}, June 29, 2001, at \url{http://www.zdnet.com/products/stories/reviews/0,4161,2621779,00.html}.
\textsuperscript{145} See \textit{id.}
\textsuperscript{146} See Polly Sprenger, \textit{Finland: Where the Wireless Are}, \textit{THE INDUSTRY STANDARD} (Jan. 7, 2000), at \url{http://www.thestandard.com/article/display/0,1151,8660,00.html}.
phone must have a special WAP phone. Only WAP phones can read the special language that is used to code a Web site. However, several companies are actively trying to eliminate this requirement by working on technologies that will deliver standard web language to mobile phones. The allure of WAP and other similar technologies is that users can connect to the Internet from virtually any location using a small mobile device instead of computers and phone lines.

With the onslaught of these developing technologies and the desirability of mobile Internet access, it is estimated that the sale of mobile Internet devices will increase to 19.2 million units by the year 2003, up from the 685,000 units sold in 1999. Wireless Internet users are expected to increase beyond the 18.1 million people currently using the wireless system, a number that has increased 187% since 1999.

There is no doubt that Internet usage will surge in the next several years, and Internet users have a variety of methods by which to access the Internet. New technologies are making access to the Internet increasingly easy and hassle-free.

4. Internet Use and Anonymity

Advances in technology have made absolute anonymity online more difficult to accomplish. With minimal effort, however, it is still relatively easy for an individual to retain some degree of anonymity on the Internet. Internet users can use various aliases or pseudonyms when online, which make it extremely difficult for law enforcement to track down offenders, or for Internet service providers to track the origin of a user, due to the sheer magnitude of Internet users.

147. See id.
148. See id. Wireless markup language (“WML”) is used to code WAP Internet sites. This is different from the traditional hypertext markup language (“HTML”), a text-based language used to construct content for the Internet.
149. Standard web language is HTML.
150. See Lake, supra note 140.
151. See Holstein, supra note 144.
152. 6.3 million people used wireless Internet access in 1999. See Lawrence, supra note 123.
154. See Greg Sandoval & Troy Wolverton, Net Crime Poses Challenges to
Additionally, Internet users can also use advances in technology, such as "remailers," or encryption software, to retain their anonymity. Remailers are Web- or software-based systems that prevent user information from being "seen" by Web sites the user is visiting. Encryption software allows users to prevent or control the release of information. For example, Public Key Encryption ("PKE") is a method by which email or other documents can be kept private from other online users, law enforcement and the government. It requires the use of encryption software installed on one's computer that scrambles and descrambles messages. PKE requires the use of two "keys," one for encrypting and the other for decrypting messages.


155. Remailers have been explained as follows:

[Remailers] are basically computers on the Internet that forward electronic mail or files to other network addresses. Before the remailer forwards the information, it strips the header from the original email so that the information showing where the message originated is no longer attached to the email. Many anonymity services replace the header with anonymous addresses. The eventual recipient of the message then has no idea about who sent the email and where it originated.


156. See Komando, supra note 153. Internet users who use major commercial Web browsers may be unaware that information about them is being shared. See id. The browser typically sends the address of the last page a user visited, information about a user's operating system, browser software, IP address, and more to each new site visited. See id. Additionally, a user's Internet service provider has the ability to track the Web sites a user has visited. See id. Internet users can use a free Web-based service called "The Anonymizer" or they can upgrade to a fee-based service that provides more privacy. See id. Additionally, users can purchase software, which they install on their own personal computer, to prevent the release of their personal information. See id.

157. See id.


159. See Friedman, supra note 158, at 213.

160. A key is a string of binary digits, the smallest unit of information on a computer. See Elinor Abreu, Universal Translator, THE INDUSTRY STANDARD (Dec. 11, 2000), at http://www.thestandard.com/article/display/0,1151,20509,00.html.
An individual has a public key, which is published so that anyone has access to it, and a private key that is kept secret by the individual. The individual encrypts a message using the "private key" and sends it to an intended recipient. The recipient receives the message and uses the sender's "public key" to unscramble the message. While individuals can conduct transactions with this method using their true names and identities, it is just as easy to use the system with an alias or pseudonym. Additionally, individuals can use an alias or pseudonym when placing their "digital signature" on an electronic document. Digital signatures are often used in conjunction with encryption software to verify the company or person with whom an individual is doing business. On October 1, 2000, Congress passed the Electronic Signatures in Global and National Commerce Act, which provides that digital signatures, or "e-signatures," have the same legal effectiveness as their ink predecessors.

5. The Senior Safety Act of 1999 and Internet Fraud

Only recently has legislation come before Congress attempting to combat fraud perpetrators who target the elderly using the Internet as their medium. The Senior Safety Act ("SSA"), as proposed, expands current telemarketing regulatory legislation by attempting to curtail the use of the Internet as a means by which telemarketers perpetrate fraud. The SSA strikes the term "telephone calls," as used in prior legislation, and replaces it with the phrase "wire communications utilizing a phone service." Although this legislation

161. Publication of a public key may occur in much the same way as telephone numbers are published in a telephone directory.
162. See Friedman, supra note 158, at 213.
163. See id.
164. A digital signature is the encrypted digest of the text in a document that accompanies an electronic message. It can be used to verify the origin of a document and to guarantee that a document has not been altered. See Abreu, supra note 160.
166. See id. § 7001(a)(1).
168. See Bratkiewicz, supra note 2, at 596.
169. S. 751 § 302(a).
may have been sufficient in the not-too-distant past to combat Internet fraud, it is almost useless today due to the surge of new technologies that provide Internet access without the use of wires or a phone service.170

III. IDENTIFICATION OF THE LEGAL PROBLEM

For the past fifteen years, Congress has made it a priority to combat telemarketing fraud.171 In 2001, the FTC was expected to issue a report to Congress regarding the effectiveness of the Telemarketing Act and Sales Rule in combating telemarketing fraud and decide to if further amendments were needed.172 In addition, Congress is currently considering two bills that would build further on the consumer protections provided by the Telemarketing Act.173 Despite these efforts to combat telemarketing fraud, Congress has done little to combat consumer fraud perpetrated via the Internet.174 Unfortunately, the same types of scams used by telemarketers have already surfaced on the Internet.175

Recognizing the potential of cyberspace, con-artists have already perpetrated several of the common telemarketing scams over the Internet.176 Solicitations for fraudulent schemes can be posted on a Web site or sent via email to an intended recipient.177 Of these two forms, perpetrators of fraud favor email because it can be targeted to a specific individual, or it can be sent in bulk to reach an innumerable

170. See discussion supra Parts II.B.2-3.
171. See Proposed Legislation, supra note 8.
172. The Telemarketing Act requires that five years after the adoption of the legislation, the FTC must review the effects of the Act and report their findings to Congress. 15 U.S.C § 6108 (1994). On February 28, 2000, the FTC published a notice in the Federal Register soliciting comments on the Telemarketing Sales Rule. See 65 Fed. Reg. 10,428 (Feb. 28, 2000). As of the publication date of this comment, the report has not yet been released.
174. See discussion infra Part II.B.
175. See Fraud Against Seniors, supra note 1.
176. For recent statistics on types of fraud perpetuated over the Internet, visit the Internet Fraud Statistics Reports section of National Fraud Information Center’s (“NFIC’s”) Web site, located at http://www.fraud.org/. The NFIC was established in 1992 by the National Consumers League, a nonprofit consumer organization.
177. See Sand, supra note 115.
amount of people.\textsuperscript{178}

Similar to telemarketing scams, current email scams include investment scams, business opportunity scams, and credit card loss protection scams.\textsuperscript{179} In addition, other email scams targeting the elderly include chain letters,\textsuperscript{180} offers for free merchandise,\textsuperscript{181} cable descrambler kits,\textsuperscript{182} guaranteed loans or credit, and vacation prize promotions.\textsuperscript{183} Email scams create a serious problem because offenders can access millions of elderly Internet users at once with minimal effort.

This access to the Internet, coupled with modern day technologies available to con-artists and the fact that there is insufficient legislation to protect against Internet fraud, has the potential to victimize millions of elderly persons. In today's world, the Internet is the fastest growing method of communication and provides the most comprehensive manner by which to reach a countless number of people.\textsuperscript{184} The widespread use of the Internet threatens to open the door even wider for criminals to conduct their illegal operations. This comment attempts to address the problems of Internet fraud specifically in conjunction with the elderly.

\textbf{IV. ANALYSIS}

Congress has recognized that telemarketing fraud poses a particular threat to elderly persons and has responded aggressively by enacting legislation to protect elderly consumers.\textsuperscript{185} But Congress has expended much less effort on combating Internet crime that targets the elderly. In order to

\textsuperscript{178} See id.


\textsuperscript{180} See id. Seniors are asked to send a small amount of money to the rest of the names on the email list they received, and then forward the message on to as many other persons as possible.

\textsuperscript{181} See id. The victim is asked to pay a fee to join a club and recruit other individuals to join. The promise is that they will receive valuable merchandise in return, which they never receive.

\textsuperscript{182} See id. Victims are asked to send money for a kit to assemble a cable descrambler and thus receive free cable access. However, the kits do not work.

\textsuperscript{183} See id. The prizes or trip offered are often grossly misrepresented or do not exist.

\textsuperscript{184} See discussion supra Part II.B.

\textsuperscript{185} See \textit{Fraud Against Seniors}, supra note 1.
INTERNET FRAUD

determine the reasons why Internet fraud threatens to replace telemarketing fraud targeting elderly persons, it is necessary to explore how the Internet and modern advances in technology affect the operation of fraudulent operations.

The SSA is the only legislation that attempts to address Internet fraud specifically targeting the elderly. While SCAMS provides penalties for telemarketing fraud against the elderly, it does not provide penalties for Internet fraud against the elderly. The SSA attempts to do so by modifying the language in SCAMS to punish individuals who use “wire communications utilizing a phone service” to carry out fraudulent activity. If enacted, this amendment would appear to expand the scope of fraud regulations concerning the elderly to include the Internet. The amendment, however, does not specifically define the Internet or its use as a proscribed method of carrying out fraud on the elderly.

A. The Use of Alternate Connection Methods and Internet Fraud

The SSA only targets fraud conducted via wire communications using a phone service. Therefore, regulation and punishment of Internet fraud targeting the elderly is limited to Internet fraud perpetrators using analog or digital phone lines to connect to the Internet.

The SSA, as proposed, does not address the problem that arises when con-artists use alternative Internet connection methods to target seniors. It is no longer necessary for fraud perpetrators to use a phone service to connect to the Internet. A popular alternative is the cable modem. Additionally, since alternative connection options are expected to essentially replace traditional analog connection systems,

---

186. See generally Bratkiewicz, supra note 2.
187. See supra Part II.A.4.b. "Telemarketing fraud" is defined as “a plan, program, promotion, or campaign that is conducted . . . by use of . . . telephone calls . . . ” 18 U.S.C § 2325 (2000).
188. As proposed, § 302 of the SSA modifies 18 U.S.C. § 2325(1)(B).
189. See Bratkiewicz, supra note 2, at 596.
190. The SSA attempts to punish those who conduct fraud through “wire communications utilizing a phone service” to carry out fraud activity. See supra note 233.
191. See Fraud Against Seniors, supra note 1.
192. See discussion supra Part II.B.2.
193. See Jones, supra note 127.
most perpetrators of Internet fraud will be using alternate connection systems. A possible result of this usage will be widespread Internet fraud scams that are not subject to the penalties provided for by the SSA.

B. The Use of Alternate Devices and Internet Fraud

Mobile telephones, PDAs, pagers, and other devices that can connect a user to the Internet allow a con-artist to perpetrate a scam from almost anywhere. It is no longer necessary for the crook to be at home in front of a desktop or laptop computer. 194 For example, an individual wishing to engage in a fraudulent operation need only have a mobile phone with Internet access. The individual could maintain a Web site and monitor responses from elderly individuals from any location, obtaining valuable credit card and other financial information. Furthermore, an individual could send mass scam emails targeting elderly persons from a mobile phone.

Even more alarming is the fact that the mobile phone is not the only way to wirelessly connect to the Internet. There are a myriad of devices and wireless connection systems that provide Internet and email access. 195 Through the use of these technologies, an individual can operate an Internet scam without violating SCAMS or the SSA. Furthermore, email and Internet scams may affect an enormous amount of elderly individuals, due to the ease and minimal cost required to set-up and maintain scams. The resulting economic losses could far surpass those resulting from telemarketing fraud. The exclusion of these technologies is a huge loophole in the legislation and one that a crafty crook may easily use to his advantage in order to continue unlawful escapades targeting seniors. Under current legislation, the deterrent effect of increased penalties for Internet fraud targeting elderly persons is nonexistent.

C. Anonymity and Internet Fraud

Additionally, the SSA does not address the problem of anonymity and Internet usage. The ability to remain anonymous on the Internet while perpetrated scams makes it ex-

194. See discussion supra Parts II.B.2-3.
195. See discussion supra Parts II.B.1-3.
tremely difficult to apprehend and punish persons carrying out these scams. This dramatically increases the potential for widespread Internet fraud because law enforcement cannot target or apprehend the perpetrators.

For example, encryption provides an attractive option for private citizens who wish to preserve their privacy online, an option that is also extremely attractive to an online con-artist. Encryption would allow con-artists to perpetrate email scams targeting seniors without being detected by law enforcement agencies. Of course, in order for this to work, both the con-artist and the elderly person would have to install encryption software on their computers. However, the increasing use of the Internet by the elderly and the growing popularity of encryption software as a means to protect individual privacy make this a cognizable possibility. The opportunity for abuse of this technology by a con-artist poses a serious threat to the elderly because the criminal can remain virtually unidentifiable by fraud watch organizations or law enforcement. Since “fraud operators are opportunistic, and therefore . . . always among the first to appreciate the potential of new technology,” they may potentially defraud indeterminable amounts of money from elderly persons without ever being caught or punished.

Additionally, Internet fraud perpetrators may easily set up an anonymous email account and use anonymous remailer to distribute hundreds, even thousands, of emails to elderly persons in order to effectuate their scam. It would be extremely difficult, if not virtually impossible, to track down the anonymous scam artist.

With the array of new technologies available to connect to the Internet, and the void of legislation that addresses Internet fraud perpetrated through these technologies, the potential for Internet fraud to run rampant is imminent. Fraudulent telemarketers who have had to cease their activities because of strict regulations by government and aggressive enforcement by law enforcement can easily realize the benefit of committing fraud on the Internet, especially if legislation

196. See Abreu, supra note 158.
197. See Friedman, supra note 205.
198. Fraud Against Seniors, supra note 1.
199. See discussion supra Part II.B.4.
only punishes wire communications fraud using phone lines. This problem is further compounded by an offender's ability to remain anonymous, their tendency to target the elderly, and the elderly's increasing use of the Internet.

V. PROPOSAL

Even elderly persons who are computer savvy may still fall prey to scams set up by clever cybercriminals. Congress, the FTC, DOJ and other law enforcement agencies must make concentrated efforts to curtail Internet fraud targeting the elderly. These efforts should take the form of new legislation, education programs for the elderly, and the use of privacy systems by the elderly to protect themselves against cybercriminals.

A. Legislation

The most effective way to reduce the possibility of victimization of elderly persons by con-artists using the Internet is to enact legislation that prohibits the use of the Internet in fraudulent operations. Specifically, the legislation should address new technologies that are used to access the Internet in lieu of the traditional modem method.

There is currently no legislation in effect that directly applies to Internet fraud perpetrators who specifically prey on the elderly. The Senior Safety Act of 1999 is a good start, but while it is pending in Congress, it must be amended to incorporate new technologies in communications. Specifically, Congress should amend the legislation to include a section on fraud conducted via the Internet, and change the language of "wire communications utilizing a telephone service" to incorporate communications that do not utilize a telephone service, such as cable modem access and wireless devices.

Furthermore, since Internet fraud poses the additional threat of potentially reaching millions of people, and new technologies make it possible to remain anonymous and perhaps undetected by law enforcement and government, Congress should consider enhancing the penalties of conviction in

200. See discussion supra Part II.A.
201. See discussion supra Parts II.B.1-3.
202. See discussion supra Part II.B.
order to deter cybercriminals from attempting to commit fraud over the Internet.

B. Education Programs

In addition to enacting legislation to address Internet fraud targeting the elderly, educational efforts to inform the elderly of fraudulent Internet activity can also aid in reducing the number of fraud victims. Although there are several Web sites that act as Internet fraud watches and warn elderly consumers about the current scams being perpetrated,\textsuperscript{203} governmental agencies should make an aggressive effort to educate elderly persons about the types of technologies that are available to con-artists and the ways in which they may use them to perpetrate fraud. Both state and federal government, as well as law enforcement agencies must participate in this educational effort.

Although Internet use among the elderly is continuously growing, AARP reports that the preferred method for gathering and learning new information is still traditional mediums, such as newspapers, magazines, books, and journals.\textsuperscript{204} The fact that elderly persons are increasingly accessing the Internet does not mandate that information regarding Internet fraud should be excluded from traditional publications. Furthermore, elderly persons who have not yet begun to use the Internet will benefit from this information as well because they will be forewarned and well-educated about Internet fraud before beginning to access the Internet. This will reduce the chances of a con-artist to take advantage of uninformed, novice Internet users.

C. The Use of Privacy Systems

Elderly persons can also protect themselves from Internet fraud by using privacy systems designed for Internet and computer use.\textsuperscript{205} These systems afford the user a means to protect their identities and important personal information.

\textsuperscript{203} In addition to the aforementioned NFIC Web site, supra note 176, other useful Web site addresses include those of the DOJ, located at http://www.usdoj.gov, and the FTC, at http://www.ftc.gov.

\textsuperscript{204} See AARP, SURVEY ON LIFELONG LEARNING (publication date 2000), available at http://research.aarp.org/general/lifelong.html.

\textsuperscript{205} See discussion supra Part II.B.3.
Two such systems are installing encryption software and using digital signatures.

1. **Encryption**

Encryption is a way for computer users to code information sent over the Internet so that it is not readily accessible to other individuals. If elderly persons use encryption software to send and receive email or to conduct transactions on the Internet, they may avoid becoming victims of Internet fraud because they can remain anonymous to fraud perpetrators. Encryption software packages are easily obtainable and can be purchased in many retail computer stores. Elderly persons, however, should be advised of the fact that Internet fraud perpetrators may also have access to encryption software, and thus the consumer may want to use additional protection methods in conjunction with encryption.

2. **Digital Signatures**

Digital signatures use encryption to provide a means for persons conducting business via the Internet to verify the identity of the company or person with whom they are doing business. This system provides verification of the origin by requiring a specific coding key which is only known by the sender of the document. Due to the increased used of the Internet in business transactions, Congress passed legislation specifically addressing the enforceability of digital signatures. This legislation gives binding effect to a business transaction "signed" with a digital signature. Elderly persons conducting business on the Internet may be protected by digital signatures not only because they can verify the company or individual with whom they are doing business, but also because the transaction is binding, making the other

---


207. See discussion supra Part II.B.3. Just as fraud perpetrators can use these systems to remain unidentifiable, the reverse is also true. Elderly persons can use the same systems to remain anonymous on the Internet.

208. See supra notes 164-66 and accompanying text.


VI. CONCLUSION

Perpetrators of fraud against the elderly have long favored telemarketing as their method of choice to carry out their operations.211 But as the government has implemented stricter regulations and enforcement provisions over the last several years, telemarketing fraud is no longer as serious a threat as it once was. Instead con-artists are turning to the Internet to carry out their scams.212 As the elderly population increasingly becomes more Internet-oriented, and new technologies continue to develop,213 the likelihood for victimization of the elderly by con-artists is imminent. The time has come to put an end to the abuse of the elderly by these con-artists.

Congress and the FTC must enact legislation and regulations encompassing all methods of accessing the Internet, and to provide clear guidance and strict penalties to combat fraud perpetrated through the Internet. Governmental as well as private agencies must make educational programs regarding computer technology and possible fraudulent operations accessible to the elderly in order to prevent the potential for widespread abuse of the senior population. Additionally, these programs should educate the elderly about technology they can utilize to protect their information and identity. Congress should take immediate action to combat Internet fraud against the elderly in order to stop the exponential increase of cybercrime.

211. See discussion supra Part II.
212. See discussion supra Part IV.
213. See discussion supra Part II.B.