06-CV-00126-CMP

ORIGINAL 02471 Summ. Iss'd.

The Honorable _____

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STATE OF WASHINGTON,

Plaintiff,

v.

SECURE COMPUTER, LLC, a New York limited liability company; PAUL E. BURKE, President of SECURE COMPUTER LLC, individually and as part of his marital community; GARY T. PRESTON, individually and as part of his marital community; MANOJ KUMAR, individually and as part of his marital community; ZHIJIAN CHEN, individually; and SETH T. TRAUB, individually, and as part of his marital community,

Defendants.

NO. C06-0126 RSL

COMPLAINT FOR INJUNCTIVE AND ADDITIONAL RELIEF UNDER THE CAN-SPAM ACT, THE UNSOLICITED COMMERCIAL EMAIL ACT, THE COMPUTER SPYWARE ACT, AND THE UNFAIR BUSINESS PRACTICES--CONSUMER PROTECTION ACT

COMES NOW, Plaintiff, State of Washington ("the State"), by and through its attorneys Rob McKenna, Attorney General; Paula Selis, Senior Counsel; and Katherine M. Tassi, Assistant Attorney General, and brings this action against Defendants named herein. The State alleges the following on information and belief:

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

I. INTRODUCTION

1.1. Plaintiff, State of Washington, brings this action under the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act"), 15 U.S.C. § 7701, *et seq.* Plaintiff seeks a permanent injunction and other equitable relief, including damages and attorneys' fees, based on Defendants' violations of the CAN-SPAM Act.

1.2 Plaintiff, State of Washington, as part of the same case or controversy, also brings this action pursuant to RCW 19.190, the Commercial Electronic Mail Act ("UCE Act"). Plaintiff seeks a permanent injunction and other equitable relief, including damages, civil penalties, and attorneys' costs and fees, based on violations of the UCE Act.

1.3 Plaintiff, State of Washington, as part of the same case or controversy, also brings this action pursuant to RCW 19.270, the Computer Spyware Act ("Spyware Act"). Plaintiff seeks a permanent injunction and other equitable relief, including damages, civil penalties, and attorneys' costs and fees, based on violations of the Spyware Act.

1.4 Plaintiff, State of Washington, as part of the same case or controversy, also brings this action pursuant to RCW 19.86, the Unfair Business Practices-Consumer Protection Act ("Consumer Protection Act"). Plaintiff seeks a permanent injunction and other equitable relief, including damages, civil penalties, and attorneys' costs and fees, based on violations of the Consumer Protection Act.

II. JURISDICTION AND VENUE

2.1 This Court has jurisdiction over this matter pursuant to 28 U.S.C. §§ 1331, 1337(a), 28 U.S.C. § 1367 and 15 U.S.C. § 7706.

2.2 Venue in this district is proper under 28 U.S.C. § 1391 and 15 U.S.C. § 7706. A substantial portion of the acts complained of herein have occurred in King County and elsewhere in the Western District of Washington.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

III. PLAINTIFF

3.1 Plaintiff, State of Washington, as *parens patriae*, is authorized by 15 U.S.C. § 7706(f) to file federal district court actions to enjoin violations of the CAN-SPAM Act, to seek recovery for actual monetary loss or damages of up to $250 per violation on behalf of the residents of the State of Washington, and to obtain such further and other relief as the Court may deem appropriate, including treble damages and attorneys' fees. Plaintiff is authorized by RCW 19.86.080 to enjoin violations of the Consumer Protection Act, to obtain restitution on behalf of persons harmed by such violations, and to obtain such further and other relief as the Court may deem appropriate, including civil penalties and attorneys' fees. Pursuant to RCW 19.190.030(2), a violation of RCW 19.190 et seq., the UCE Act, constitutes a violation of the Consumer Protection Act and thereby gives rise to Plaintiff's authorization to file actions enjoining violations of the UCE Act and to seek damages of $500 per violation of its provisions. Pursuant to RCW 19.270.060, the Spyware Act, Plaintiff is authorized to seek recovery for actual monetary loss or damages of up to $100,000.00 per violation of RCW 19.270 on behalf of the residents of the State of Washington, and to obtain such further and other relief as the Court may deem appropriate, including treble damages and costs and attorneys' fees.

IV. DEFENDANTS

4.1 Defendant Secure Computer, LLC ("SCL") is a New York limited liability company. Defendant SCL is located at 81 Main St. Suite 303, White Plains, New York 10601. Since at least July 2004, SCL has developed, advertised, promoted, and sold various software products to the public over the Internet, including a product called Spyware Cleaner, a purported anti-spyware program that detects and cleans spyware from the user's computer, and a product called Error Fixer, which purportedly repairs the registry files of the user's computer. SCL owns, operates, and controls several Web sites, including www.myspywarecleaner.com, www.myerrorfixer.com, and www.checkforspyware.com. SCL uses these Web sites, as well

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

as hundreds of other Web sites, to market, advertise, and sell software products, and to recruit consumers for its affiliate advertising program. SCL transacts or has transacted business in the state of Washington and in the Western District of Washington.

4.2 Defendant Paul E. Burke ("Burke") is the president of Secure Computer, LLC, and as such, controls its policies, activities, and practices, including those alleged in the Complaint herein. Burke is married to Wendy Burke and together they constitute a marital community. Defendant resides at 622 Richbell Road, Apt. C, Larchmont, NY 10538, and at 3755 Henry Hudson Parkway W, Apt. 8H, Bronx, NY 10463. All acts and practices undertaken by Burke on behalf of SCL are and were for the benefit of his marital community. Defendant resides in the state of New York and transacts or has transacted business in the state of Washington and in the Western District of Washington.

4.3 Defendant Gary T. Preston ("Preston") is married to Jane Doe Preston, and together they constitute a marital community. Preston is the registrant, that is, the owner of, and administrative and technical contact for, the Web sites www.myspywarecleaner.com and www.securecomputerllc.com, the Web domain for SCL. As such, he controls the policies, activities, and practices of SCL. Preston resides at 14110 82nd Dr., Apt 433, Jamaica, NY 11435-1105. All acts and practices undertaken by Preston on behalf of SCL are and were for the benefit of his marital community. Defendant resides in the state of New York and transacts or has transacted business in the state of Washington and in the Western District of Washington.

4.4 Defendant Manoj Kumar ("Kumar") is an affiliate advertiser of SCL's software product Spyware Cleaner. Defendant is married to Jane Doe Kumar and together they constitute a marital community. Defendant resides at 76-Venkatagiri, Anushakti Nagar, BARC Colony, Mumbai-400094, Maharashtra, India. Kumar promotes, markets, and advertises Spyware Cleaner through unsolicited commercial electronic mail ("email") sent to residents

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

across the United States, including residents in Washington State and in the Western District of Washington. All acts and practices undertaken by Kumar are and were for the benefit of his marital community.

4.5 Defendant Zhijian Chen ("Chen") is an affiliate advertiser of SCL's software product Spyware Cleaner. Chen is married to Jane Doe Chen and together they constitute a marital community. Defendant resides at 8642 SE Rhone St., Portland, OR 97266. Defendant promotes, markets, and advertises Spyware Cleaner through net send messages sent to the computers of residents across the United States, including residents in Washington State and in the Western District of Washington. All acts and practices undertaken by Chen are and were for the benefit of his marital community.

4.6 Defendant Seth T. Traub ("Traub") is an affiliate advertiser of SCL's software product Spyware Cleaner. Traub is married to Jane Doe Traub and together they constitute a marital community. He resides at 909D State Street, Portsmouth, NH 03801. Traub promotes, markets, and advertises Spyware Cleaner through advertisements on the Web site Google.com to computer users across the United States, including residents in Washington State and in the Western District of Washington. All acts and practices undertaken by Traub are and were for the benefit of his marital community.

V. NATURE OR TRADE OF COMMERCE

5.1 SCL, Burke, Preston, Kumar, Chen, and Traub (collectively, "Defendants") promote, advertise, market, and sell a purported anti-spyware software called Spyware Cleaner to consumers across the United States, including consumers located in Washington State, over the Internet. As part of their marketing efforts, SCL, Burke, and Preston operate the Web site www.myspywarecleaner.com. The Web site allows consumers to purchase Spyware Cleaner over the Internet. SCL, Burke, and Preston also advertise their product using the services of digital marketing and ad-serving companies, such as Fast Click, Burst Media, AdTegrity, and

Oridian. These companies assisted SCL, Burke, and Preston in publishing and serving advertisements for Spyware Cleaner to Web sites and in tracking data regarding the success of the advertisements, in piquing consumer interest, and in sales of the product. Defendants created pop-up, pop-under, and banner advertisements, all of which have appeared on hundreds of Web sites across the country, including, for example, www.celebguru.com ("Celebrity Guru"), a Web site devoted to celebrity biographies, and on numerous Washington-based Web sites.

5.2 On their own Web site for Spyware Cleaner, SCL, Burke, and Preston also solicit consumers to become affiliate advertisers of Spyware Cleaner, which involves marketing the product in return for a commission for each sale of the product that results from the affiliate's advertisement. Affiliates can advertise in various ways, including displaying advertisements for Spyware Cleaner on their own Web site, displaying advertisements on other Web sites, or direct marketing through electronic mail. Once a consumer signs up to be an affiliate advertiser of Spyware Cleaner, SCL, Burke, and Preston offer to the affiliates visual images, along with HTML code for the images, of advertisements for Spyware Cleaner. These advertisements are substantially similar to those advertisements that SCL, Burke, and Preston use in advertising their product themselves. Spyware Cleaner is also marketed and sold through an affiliate network marketplace called Click Bank, which is owned and managed by Click Sales, Inc. Spyware Cleaner is featured in the Click Bank marketplace catalogue. Someone who is interested in promoting Spyware Cleaner in return for a commission on the sale of the product registers with Click Bank to become an affiliate. Click Bank then directs the consumer to www.myspywarecleaner.com and the consumer registers with SCL to begin marketing the product. As with affiliates who sign up directly with SCL, SCL gives Click Bank affiliates a choice of numerous advertisements to use, all substantially similar to those the SCL, Burke, and Preston use themselves. For every sale of Spyware Cleaner that is made

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

as a result of the affiliate's advertising, the affiliate is paid a percentage of the purchase price. SCL offers affiliates of the Click Bank marketplace 75% of the $49.95 purchase price of Spyware Cleaner.

5.3 Kumar, Chen, and Traub are all Click Bank affiliate advertisers of Spyware Cleaner. Each of these Defendants advertises and markets, or has advertised and marketed, Spyware Cleaner in return for a commission on the sale of the product. Kumar advertises, promotes, and markets Spyware Cleaner through unsolicited commercial emails that contain a hyperlink to SCL's Web site, www.myspywarecleaner.com. Chen advertises, promotes, and markets Spyware Cleaner through net send messages sent to users' computers. Net send is a Windows operating system command that is used to send messages to a computer system or to a group of computer systems where Windows Messenger service is running. The net send command will send a message to users' computers and a pop-up dialogue box will appear on their screen. In the past, the net send command was often used for broadcast messages by network administrators such as "email server down." However, net send messages can also be used as a way to send unsolicited messages to unsuspecting users. A net send command can send a dialogue box with an advertisement to millions of computers. Traub advertises, promotes, and markets Spyware Cleaner through advertisements on Google.com. Traub's advertisement is in the form of a hyperlink with the headline "Microsoft Spyware Cleaner," which appears as a sponsored, that is, paid for, link when certain search terms are entered in the search field on Google.com, including the search terms "Microsoft anti-spyware," "Microsoft antispyware," and "Microsoft spyware cleaner." When Traub's hyperlinked headline is clicked on, the user is taken to www.myspywarecleaner.com rather than to a Microsoft anti-spyware product site. Each of these Defendants receives, or has received, a commission of 75% of the $49.95 purchase price for each sale of Spyware Cleaner that his advertisement generates or has generated.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

5.4 Defendants are in competition with others in the State of Washington engaged in a similar business.

VI. VIOLATIONS OF THE CAN-SPAM ACT

(Defendants Kumar, SCL, Burke, and Preston)

A. First Cause of Action: False Headers

6.1. Plaintiff realleges paragraphs 1.1 through 5.4 and incorporates them herein as if set forth in full.

6.2 The CAN-SPAM Act makes it unlawful to initiate the transmission of an email that contains materially misleading or materially false header information. 15 U.S.C. § 7704(a)(1). The term "materially" includes the alteration or concealment of header information that would impair the ability of a law enforcement agency, among other entities, to identify the initiator of the email message or to investigate an alleged violation of the Act. 15 U.S.C. § 7704(a)(6). The Act also makes it unlawful to initiate email with misleading subject lines. 15 U.S.C. § 7704(a)(2). Additionally, the Act requires senders of commercial electronic mail to provide a functioning mechanism by which recipients can opt out of receiving future emails from the sender, and makes it unlawful to send additional solicitations to those who have opted out. 15 U.S.C. § 7704(a)(4)(A). Once a recipient requests not to receive future commercial electronic mail messages from the sender, the sender has a 10-day grace period after which it is unlawful to send any messages to that recipient. 15 U.S.C. § 7704(a)(4)(A)(i). The Act also requires commercial electronic mail to contain conspicuous notice that the message is an advertisement and conspicuous notice of the recipient's right to opt out of receiving further email messages. 15 U.S.C. § 7704(a)(5)(A)(i),(ii). The Act also requires that the email message contain a valid postal address. U.S.C. § 7704(a)(5)(A)(iii). The term "initiate" means "to originate or transmit" or "to procure the origination or transmission of" a commercial electronic message. 15 U.S.C. §

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

7702(9). The term "procure" means to intentionally pay or provide other consideration to another to initiate a commercial electronic message. 15 U.S.C. § 7702(12).

6.3 Kumar has altered or concealed header information in his unsolicited commercial email that promotes and advertises Spyware Cleaner. Kumar posts in the "From" line of his email messages: "MSN Member Services." In fact, the sender address is false since Kumar is not employed by MSN and the email was not sent by MSN Member Services. By using such a sender line, Defendant has initiated the transmission of commercial electronic mail messages with materially misleading or materially false header information, thus impairing the ability of recipients of the email, including Plaintiff, to identify and locate the initiator of the email. "Header information," as defined in the Act, means "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." 15 U.S.C. § 7702(8).

6.4 SCL, Burke, and Preston entered into a contract with Click Bank to sell Spyware Cleaner by means of Click Bank's extensive affiliate network. SCL, Burke, and Preston have earned over $100,000.00 from sales through Click Bank's affiliates, including Kumar. SCL, Burke, and Preston procured, and thereby initiated, the transmission of commercial electronic mail messages with materially misleading or materially false header information, thus impairing the ability of recipients of the email, including Plaintiff, to identify and locate the initiator of the email. 15 U.S.C. § 7704(a)(1).

6.5 The practices described above constitute violations of 15 U.S.C. § 7704(a)(1).

B. Second Cause of Action: Deceptive Subject Lines

6.6 Plaintiff realleges paragraphs 1.1 through 6.5 and incorporates them herein as if set forth in full.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

6.7 Kumar's commercial email messages display the subject line: "Special Security Alert for MSN Members." This subject line creates the false and misleading impression that the email concerns an actual security issue that MSN is communicating to its members. The use of this subject line in conjunction with the sender address of "MSN Member Services" creates the false impression that the message has been sent by security-related personnel at MSN. Additionally, the use of the term "alert" implies that the message is of a high priority and requires immediate attention. The subject line is likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message. The message in fact is commercial in nature and contains an advertisement for Spyware Cleaner.

6.8 SCL, Burke, and Preston entered into a contract with Click Bank to sell Spyware Cleaner by means of Click Bank's extensive affiliate network. SCL, Burke, and Preston have earned over $100,000.00 from sales through Click Bank's affiliates, including Kumar. SCL, Burke and Preston have procured, and thereby initiated, the transmission of commercial electronic mail messages with materially misleading subject lines. 15 U.S.C. § 7704(a)(2).

6.9 The practices described above constitute violations of 15 U.S.C. § 7704(a)(2).

C. Third Cause of Action: Failure To Provide Opt-Out Mechanism

6.10 Plaintiff realleges paragraphs 1.1 through 6.9 and incorporates them herein as if set forth in full.

6.11 Kumar's email solicitation does not provide a functioning mechanism, clearly and conspicuously displayed, that a recipient may use, in a manner specified in the message, to request not to receive further messages from the sender.

6.12 SCL, Burke and Preston have procured, and thereby initiated, the transmission of commercial electronic mail messages that do not provide a functioning mechanism, clearly and conspicuously displayed, that a recipient may use, in a manner specified in the message, to request not to receive further messages from the sender.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

6.13 The practices above constitute a violation of 15 U.S.C. § 7704(a)(3)(A).

D. Fourth Cause of Action: Failure To Identify Message as Advertisement

6.14 Plaintiff realleges paragraphs 1.1 through 6.13 and incorporates them herein as if set forth in full.

6.15 Kumar's email solicitation does not identify itself clearly and conspicuously as an advertisement.

6.16 The CAN-SPAM Act requires initiators of commercial electronic mail to provide clear and conspicuous identification of the message as an advertisement. 15 U.S.C. § 7704(a)(4)(A). Kumar's electronic mail messages fail to provide clear and conspicuous notice that the mail is an advertisement, which constitutes a violation of 15 U.S.C. § 7704(a)(4)(A)(i).

6.17 SCL, Burke and Preston have procured, and thereby initiated, the transmission of commercial electronic mail messages that do not provide clear and conspicuous notice that the mail is an advertisement, which constitutes a violation of 15 U.S.C. § 7704(a)(4)(A)(i).

E. Fifth Cause of Action: Failure To Provide Notice of Option to Opt-Out

6.18 Plaintiff realleges paragraphs 1.1 through 6.17 and incorporates them herein as if set forth in full.

6.19 Kumar's email solicitation does not provide clear and conspicuous notice of the recipient's opportunity 15 U.S.C. § 7704(a)(3)(A) to decline to receive further email messages from the sender.

6.20 The CAN-SPAM Act requires initiators of commercial electronic mail to provide clear and conspicuous notice of the recipient's opportunity under 15 U.S.C. § 7704(a)(3)(A) to decline to receive further email messages from the sender.

6.21 Kumar's failure to provide in his commercial email messages clear and conspicuous notice of the recipient's opportunity under 15 U.S.C. § 7704(a)(3)(A) to decline to

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

receive further email messages from the sender constitutes a violation of 15 U.S.C. § 7704(a)(4)(A)(ii).

6.22 SCL, Burke and Preston have procured, and thereby initiated, the transmission of commercial electronic mail messages that do not provide clear and conspicuous notice of the recipient's opportunity under 15 U.S.C. § 7704(a)(3)(A) to decline to receive further email messages from the sender, which constitutes a violation of 15 U.S.C. § 7704(a)(4)(A)(ii).

F. Sixth Cause of Action: Failure To Include Physical Address of Sender

6.23 Plaintiff realleges paragraphs 1.1 through 6.22 and incorporates them herein as if set forth in full.

6.24 Kumar's email solicitation does not provide a physical postal address.

6.25 The CAN-SPAM Act requires initiators of commercial electronic mail to provide a physical postal address in the message. 15 U.S.C. § 7704(a)(4)(A)(iii).

6.26 Kumar's failure to provide a physical postal address in his commercial electronic mail constitutes a violation of 15 U.S.C. § 7704(a)(4)(A)(iii).

6.27 SCL, Burke and Preston have procured, and thereby initiated, the transmission of commercial electronic mail messages that do not provide a physical postal address, which constitutes a violation of 15 U.S.C. § 7704(a)(4)(A)(iii).

VII. VIOLATIONS OF WASHINGTON'S COMMERCIAL ELECTRONIC MAIL ACT

(Defendant Kumar)

A. Seventh Cause of Action: Misrepresenting the Point of Origin

7.1 Plaintiff realleges paragraphs 1.1 through 6.27 and incorporates them herein as if set forth in full.

7.2 Defendant Kumar's email purports in the header "from" line to originate from MSN Member Services. Kumar is not affiliated in any way with MSN. In fact, some of his email

has originated from an Internet Protocol address in India, where Kumar resides. Defendant's emails have been sent to Washington residents, including, but not limited to, MSN email account holders.

7.3 The UCE Act prohibits misrepresenting or obscuring any information in identifying the point of origin or the transmission path of a commercial electronic mail message. RCW 19.190.020(1)(a). By engaging in the practices described in paragraph 7.2, Defendant has misrepresented or obscured the transmission paths of commercial email messages and thereby violated the UCE Act. A violation of the UCE Act constitutes a *per se* violation of the Consumer Protection Act. RCW 19.190.030(3).

B. Eighth Cause of Action: Misleading Subject Lines

7.4 Plaintiff realleges paragraphs 1.1 through 7.3 and incorporates them herein as if set forth in full.

7.5 Defendant's commercial email messages display the subject line: "Special Security Alert for MSN Members." This subject line creates the false and misleading impression that the email concerns an actual security issue that MSN is communicating to its members. The use of this subject line in conjunction with the sender address of "MSN Member Services" creates the false impression that the message has been sent by security-related personnel at MSN. Additionally, the use of the term "alert" implies that the message is of a high priority and requires immediate attention. The subject line is likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message.

7.6 The use of false or misleading information in the subject line of a commercial email message violates RCW 19.190.030(1)(b). Pursuant to RCW 19.190.030(2), Defendant's violation of RCW 19.190.030(1)(b) constitutes a *per se* violation of the Consumer Protection Act, RCW 19.86, et seq.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

VIII. VIOLATIONS OF THE SPYWARE ACT

A. Ninth Cause of Action: Inducing Computer Users To Install Software for Security Purposes -- Defendants SCL, Burke and Preston

8.1 Plaintiff realleges paragraphs 1.1 through 7.6 and incorporates them herein as if set forth in full.

8.2 Since at least 2004, SCL, Burke, and Preston, through a variety of means, have advertised, marketed, and sold a computer software program known as Spyware Cleaner. Spyware Cleaner is a purported anti-spyware program that supposedly will detect and rid a user's computer of spyware. Among other means, Spyware Cleaner is advertised through pop-up and pop-under advertisements that appear on Web sites during a user's browsing session. These advertisements are served to the Web sites via Internet ad servers, including ad servers controlled by the companies Right Media, Inc. and Burst! Media, Inc. For example, Defendants disseminate, and cause to be disseminated, advertisements for Spyware Cleaner on the Celebrity Guru Web site. On this Web site, devoted to information about celebrities, when a user clicks on a hyperlink to take them to information about a particular celebrity, Defendants' pop-up advertisement appears. Defendants also disseminate, and cause to be disseminated, advertisements for Spyware Cleaner on a number of Washington-based Web sites, along with hundreds of other Web sites around the country.

8.3 The pop-up and pop-under advertisements that appear on various Web sites warn users that their computers may be infected with dangerous spyware and that immediate removal may be required. Defendants' advertisements simulate Microsoft Windows security dialogue boxes, with a blue border and a grey interior. Figure 1 depicts one advertisement for Spyware Cleaner.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

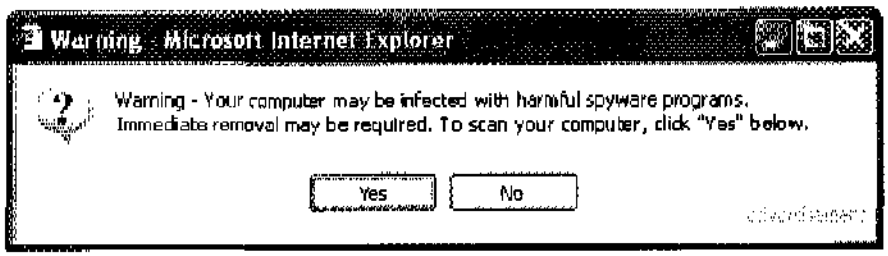


Figure 1.

Such dialogue boxes are familiar to any computer user. The only signal that the pop-up or pop-under is, in fact, an advertisement is a faint impression of the word "advertisement" in the lower right-hand corner of the dialogue box, a word that can barely be seen against the grey background. Disguised as a security warning claiming that a user needs to scan their computer for security reasons because "[i]mmediate removal may be required," Defendants' advertisements induce the user to get a "free scan" of their computer, which downloads software to their computer, to determine if it is infected with spyware.

8.4 When the user clicks on the button to get a free scan, a new browser window opens on the user's computer and Defendants' Web site, www.myspywarecleaner.com, launches. On their site, Defendants instruct the user on how to download the "free scanner." Defendants again warn the user of the potential immediate threat of spyware on their computer and encourage the user to click on a hyperlink to scan their computer. Figures 2 and 3 are images from the www.myspywarecleaner.com Web site.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

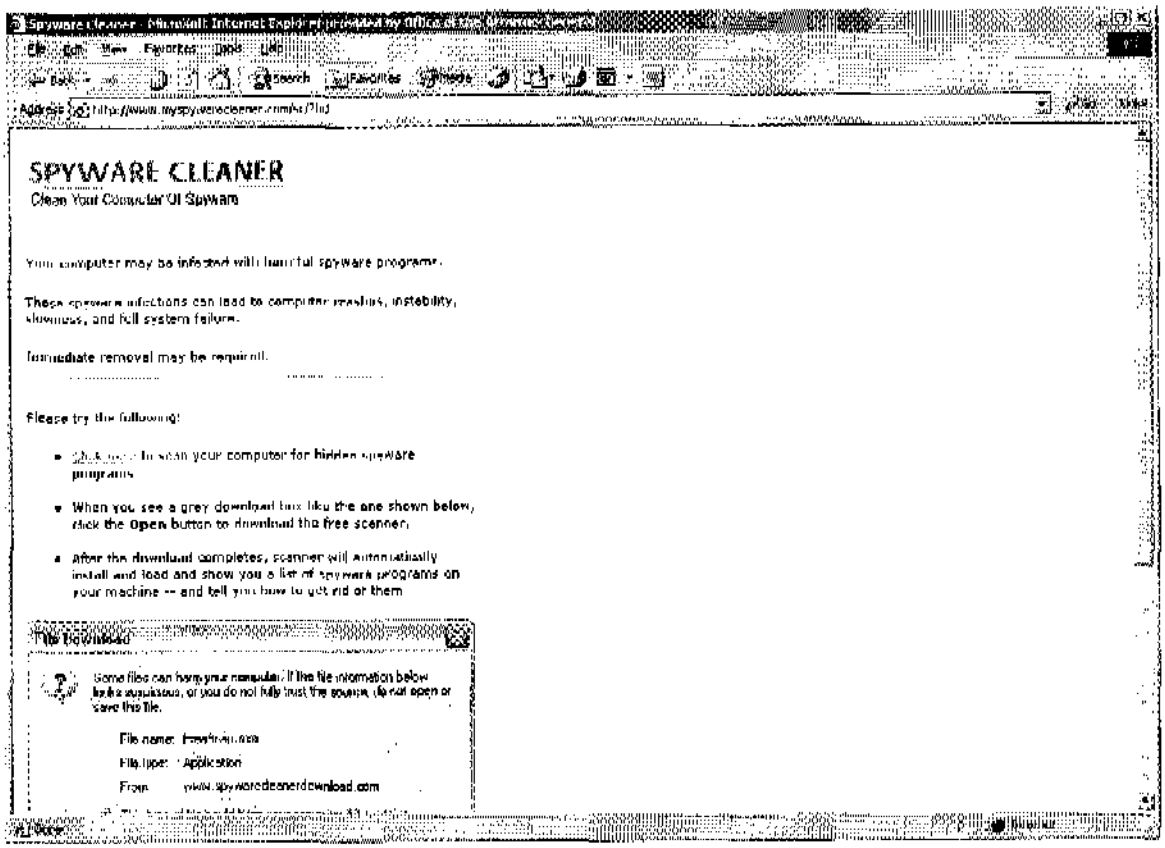


Figure 2.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

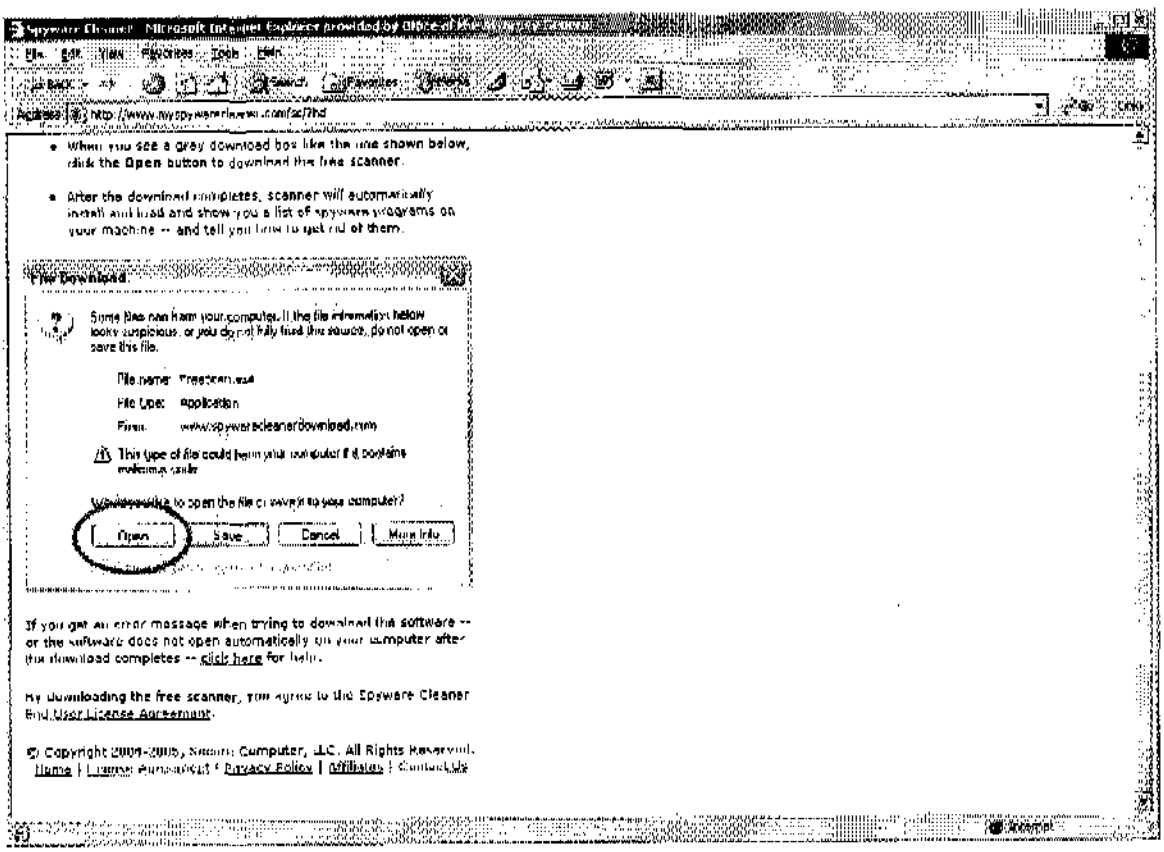


Figure 3.

Defendants inform the user that the "free scanner" will download and install; however, Defendants' advertisement does not disclose that if the user clicks on the option to run the free scan of their computer, it is not only a free scanner that will download, but, rather, Defendants' "Spyware Cleaner" software will in fact download, install itself on the user's computer, and execute automatically, all without the user's knowledge, permission, or input. Defendants mislead the user into believing that they are only downloading a free scanner, something that is different from anti-spyware software. In fact, Defendants' complete Spyware Cleaner software program is downloaded and installed during the "scan".

8.5 After the user clicks on the hyperlink to get a free scan, the user then watches as the scan results appear on the screen. The scan always detects "spyware," even when there is not, in fact, any spyware or any other harmful files on the user's computer. Rather than

detecting any actual spyware, Defendants' software program in fact labels ordinary Windows system registry keys as "BonzaiBuddy" "extreme risk" spyware. Typical results of a scan of a computer that is free from spyware are depicted in Figure 4.

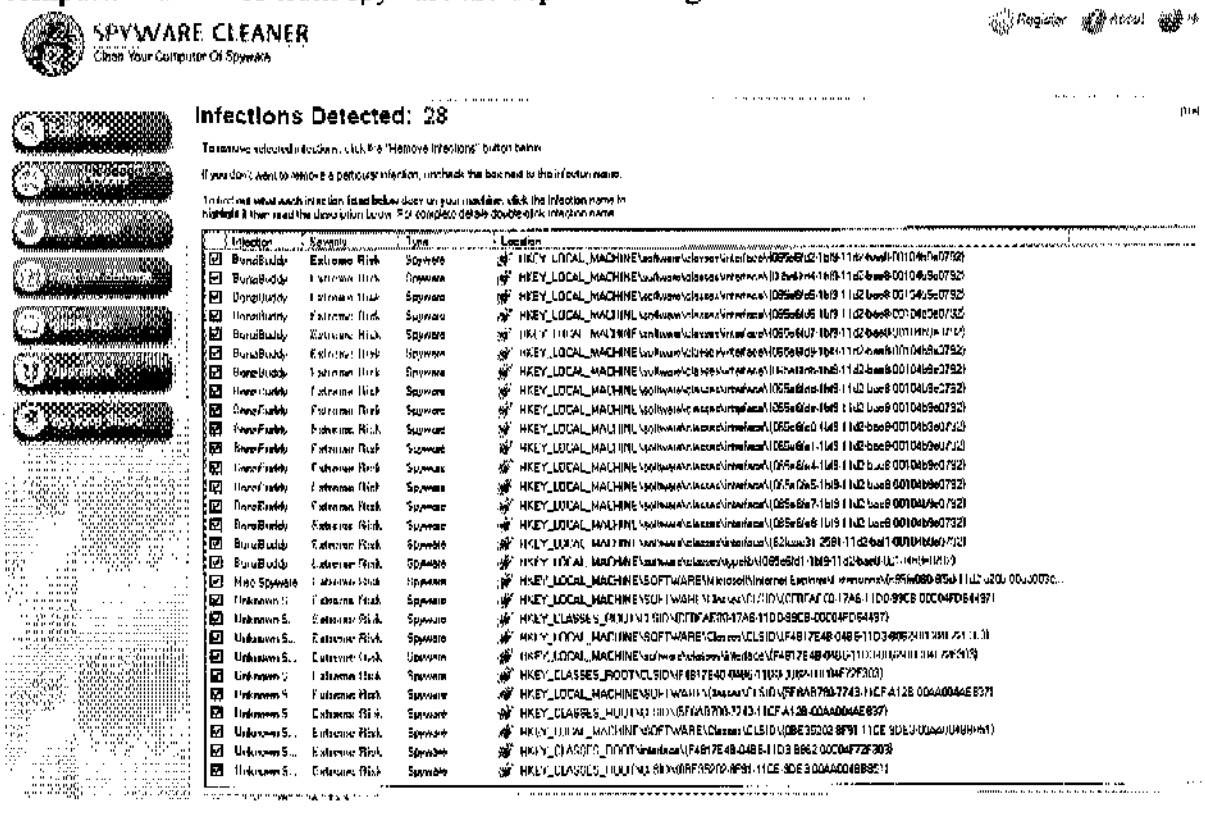


Figure 4.

8.6 Beneath the scan results is a button for the user to click to remove the alleged infections on their computer. When the user clicks on the button, Defendants reveal that in order to clean their computer of the spyware, the user must purchase the full Spyware Cleaner program. At this point in the process, Defendants claim that every moment the user leaves the spyware on their computer the spyware could be doing damage. Deceived into believing that dangerous spyware is on their computer and there is no time to waste, the user is induced to purchase Spyware Cleaner. In order to purchase Spyware Cleaner, which is sold for $49.95, the user must submit personally identifiable information, such as a credit card number and the bank from which the credit card is issued over a non-secured Web site. After the user has

purchased Spyware Cleaner, Defendants send the user an email with a registration code. The user then returns to www.myspywarecleaner.com -- or, when the user re-boots their computer, the Web site automatically launches -- and clicks on the button to remove infections. The software program that has already been installed performs another scan, reveals the same infections as it did during the free scan, and then allegedly removes the spyware from the user's computer.

8.7 Defendants intentionally and knowingly use deceptive means to alarm users that their computers may be infected with dangerous spyware and thereby induce the user to download software by claiming the software is necessary to secure the user's computer. Further, the free scan falsely reports the presence of alleged high-risk spyware, thereby inducing the user to purchase Spyware Cleaner as necessary for the security of their computer. Defendants thereby induce the user to install the Spyware Cleaner software onto their computer by claiming that the software is necessary for security reasons.

8.8 The practices described above constitute violations of RCW 19.270.040(1), which makes it unlawful for a person who is not an owner or operator of a user's computer to induce an owner or operator to install a computer software component onto the computer by intentionally misrepresenting the extent to which installing the software is necessary for security.

B. Tenth Cause of Action: Inducing Computer Users To Install Software for Security Purposes – Defendant Chen

8.9 Plaintiff realleges paragraphs 1.1 through 8.8 and incorporates them herein as if set forth in full.

8.10 Since around May 2005, Defendant Chen, has promoted, marketed, advertised and sold Spyware Cleaner through net send messages. Chen is an affiliate advertiser and promoter of Spyware Cleaner with the affiliate network Click Bank. He has been paid

thousands of dollars in commissions for the advertisement and sale of Spyware Cleaner. SCL, Burke, and Preston derive financial benefit from Chen's advertising, and Chen derives financial benefit from the sale of the product.

8.11 Defendant Chen has transmitted or caused to be transmitted to users' computers advertisements for Spyware Cleaner using net send messages. Chen's net send message pops up onto a user's computer whether or not the user is connected to the Internet and alarms the user by claiming that their computer has a virus or spyware on it. One message states: "Message from SYSTEM to ALERT... Warning! We detected a virus on your computer! We were unable to remove it automatically so please visit http://www.fixscan.com and download our software to remove Adware, Spyware and Viruses from your computer!" The message tells the user that the virus allows companies to spy on their Internet use and then recommends that the user go to a hyperlinked site to install software to remove the virus. When the user clicks on the hyperlink for www.fixscan.com, the user is taken to www.myspywarecleaner.com, where the user has the same experience as described in this section in paragraphs 8.4 through 8.7. Defendant Chen thereby induces the user to install the Spyware Cleaner software onto their computer by claiming that their computer is infected with spyware or viruses. Defendant Chen has been paid 75% of the purchase price for each sale of Spyware Cleaner generated by his advertisements.

8.12 Defendant Chen intentionally and knowingly uses deceptive means to alarm users that their computers may be infected with dangerous spyware and thereby induces the user to download software by claiming the software is necessary to secure the user's computer.

8.13 The practices described above constitute violations of RCW 19.270.040(1), which makes it unlawful for a person who is not an owner or operator of a user's computer to induce an owner or operator to install a computer software component onto the computer by

intentionally misrepresenting the extent to which installing the software is necessary for security.

C. Eleventh Cause of Action: Modifying Security Settings -- Defendants SCL, Burke, and Preston

8.14 Plaintiff realleges Paragraphs 1.1 through 8.13 and incorporates them herein as if set forth in full.

8.15 When the user elects to get a "free scan" of their computer, the Spyware Cleaner software not only automatically downloads, installs, and executes, but it surreptitiously erases the contents of the Windows operating system Hosts files. Such modification of the user's operating system is without any legitimate purpose.

8.16 Simply put, a Hosts file, which is stored on the computer's file system, is like an address book. When the user types an address like www.google.com into their browser, the Hosts file is consulted to see if the user has the Internet Protocol ("IP") address, or "telephone number," for that site. If the user has the IP address, then their computer will "call it" and the site will open. If not, their computer will ask their ISP's (internet service provider) computer for the phone number before it can "call" that site.

8.17 One use of the Hosts file is for ad-filtering. A user can block an ad server by adding a line to the Hosts file that maps the ad server's host name to 127.0.0.1 (home IP) or 0.0.0.0 (no IP). Then, when an Internet-capable program attempts to contact the advertiser, its request is rerouted and no advertisement can be loaded. Since no additional programs are necessary to do this, Hosts file-based ad-blocking is an extremely simple form of Internet security; it requires no loading time and takes up no memory on the user's computer. If a user wants to block an advertiser, the user simply right clicks on the banner or advertisement and clicks on properties. This will give the user the URL (Web address) needed to add to the computer's Hosts file.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

8.18 Another use of the Hosts file is for security purposes to combat spyware and virus authors' use of Hosts files for malicious purposes. Just as the Hosts file can be used to redirect advertising servers to dummy ones, a spyware program can redirect popular Web sites to an advertiser's server. This technique is known as hijacking. As a security measure, realtime-monitoring software such as Microsoft AntiSpyware "Hosts Monitor" warns a user if anything attempts to edit the Hosts file. Commercial antispyware software like ZoneAlarm and Spybot - Search & Destroy have a feature to "lock" the Hosts file. Computer owners can use the Hosts file to block traffic to their computer from Web sites that are known to expose computers to spyware, adware, and other malicious programs. See *Blocking Unwanted Sites With a Hosts File*, (visited Jan. 11, 2006) <http://www.mvps.org/winhelp2002/hosts.htm>. A software program that wipes out the Hosts file therefore damages the computer, rendering it vulnerable to spyware and virus installations.

8.19 When Defendants induce a user to get a "free scan" of their computer for spyware, the software that downloads, installs, and executes to produce the false scan results also erases the contents of the user's Hosts file. Any malicious Web sites that the user has put in their Hosts file to secure their computer from spyware, adware, or viruses may be wiped out, and the user's machine is damaged and left vulnerable, unbeknownst to the user.

8.20 Defendants induce the user to run a "free scan" of their computer through false representations and thereby transmit software to the user's computer that modifies a security setting on the computer.

8.21 The practices described above constitute violations of RCW 19.270.030(2)(b), which makes it unlawful for a person who is not an owner or operator of a user's computer to transmit computer software with actual knowledge or with conscious avoidance of actual knowledge and to use the software to modify any of the computer's security settings related to the user's access to, or use of, the Internet.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

IX. VIOLATIONS OF WASHINGTON'S CONSUMER PROTECTION ACT

A. Twelfth Cause of Action: Misrepresentations – Defendants SCL, Burke, and Preston

9.1 Plaintiff realleges paragraphs 1.1 through 8.21 and incorporates them herein as if set forth in full.

9.2 In the context of their advertising, promotion, marketing, and sale of Spyware Cleaner, SCL, Burke, and Preston make numerous misrepresentations, including, but not limited to, the following:

9.2.1 Defendants SCL, Burke, and Preston advertise Spyware Cleaner by means of pop-up and pop-under advertisements that simulate Windows or Internet Explorer dialogue boxes with a warning message. The pop-ups do not identify a product but merely appear as warning messages stating that the user's computer may be infected with harmful spyware or that their computer's registry files might contain critical errors and that immediate removal or attention may be required. Defendants represent that the user's computer is in danger. In fact, the user's computer is at no specific risk when the pop-up or pop-under appears.

9.2.2 Defendants SCL, Burke, and Preston represent that Spyware Cleaner is available at a discounted price if the user purchases the program the day that the user goes to their Web site. The Web site states: "If you register by [fill in whatever date the user goes to this Web page], you will get an entire year of unlimited use and we will slash the price from $69.95 to only $49.95." In fact, Defendants have priced the product at $49.95, so whatever day a user goes to that Web page, they will be offered the product at the "discounted price."

9.2.3 Defendants SCL, Burke, and Preston represent that Spyware Cleaner is an effective spyware-removal program and will protect the user's computer from spyware. In fact, the product does not clean the user's computer of virtually any actual spyware.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

9.2.4 *Defendants' advertisements simulate* a Microsoft Windows dialogue box with the Internet Explorer icon and a warning message. The advertisements fail to display the word "advertisement" in an obvious manner and the fail to disclose the product being advertised. In this way, Defendants represent that their advertisement is an actual warning originating from the Microsoft Windows operating system regarding spyware on their computer. In fact, Defendants' pop-ups are commercial advertisements for Spyware Cleaner and are not associated in any way with the user's Microsoft Windows operating system.

9.3 The misrepresentations described above constitute unfair and deceptive acts or practices in trade or commerce and unfair methods of competition in violation of the Consumer Protection Act, RCW 19.86.020.

B. Thirteenth Cause of Action: Misrepresentations – Defendant Chen

9.4 Plaintiff realleges paragraphs 1.1 through 9.3 and incorporates them herein as if set forth in full.

9.5 In the context of his advertising, promotion, and marketing of Spyware Cleaner, Chen represents in his net send messages that the user's computer is infected with spyware or a virus; in fact, the user's computer is not infected with spyware or viruses, and Chen's net send messages are nothing more than advertisements for an undisclosed product. Defendant Chen advertises Spyware Cleaner through net send messages that appear spontaneously on a user's computer. One of Chen's advertisements states: "Message from SYSTEM to ALERT... Warning! We detected a virus on your computer! We were unable to remove it automatically so please visit *http://www.fixscan.com* and download our software to remove Adware, Spyware and Viruses from your computer!" The message tells the user that the virus allows companies to spy on their Internet use and then recommends that the user go to a hyperlinked site to install software to remove the virus. When the user goes to the Web site listed on the message, the user is directed to www.myspywarecleaner.com. Defendant's representation has

the capacity to deceive the user into believing that their computer is infected with a virus and increases the likelihood that the user will purchase the product.

9.6 The practices described above constitute an unfair and deceptive act or practice in trade or commerce and an unfair method of competition in violation of the Consumer Protection Act, RCW 19.86.020.

C. Fourteenth Cause of Action: Misrepresentations – Defendant Kumar

9.7 Plaintiff realleges paragraphs 1.1 through 9.6 and incorporates them herein as if set forth in full.

9.8 In the context of his advertising, promotion, marketing, and sale of Spyware Cleaner, Kumar makes numerous misrepresentations, including, but not limited to, the following:

9.8.1 Kumar represents in his email advertisements that the email originates from MSN Member Services. Kumar posts in the "From" line of his email message: "MSN Member Services." Kumar has sent his email solicitations to MSN email account holders. The effect of this "From" line is deceptive. The recipient believes that the email message originates from the MSN and that it concerns their account. The misrepresentation greatly enhances the chance that the user will read the email and purchase the product. In fact, the message is not from MSN and does not concern their email account but instead is a commercial solicitation.

9.8.2 Kumar represents in the subject line of his email message that the message is a security alert for MSN members. The subject line reads: "Special Security Alert for MSN Members." The effect of this subject line is deceptive. Coupled with the "from" line reading "MSN Member Services," the subject line leads the recipient to believe that the email message originates from MSN and that it contains a security alert concerning their account. The misrepresentation greatly enhances the chance that the user will read the email and that the user will purchase the product. In fact, the message is not from MSN and does not concern a security alert regarding their email account but instead is a commercial solicitation.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

9.8.3 Kumar represents in the body of his email advertisement that the message is from Microsoft. In fact, Kumar is not affiliated with Microsoft and the message is not from Microsoft. Defendant's email displays the word "Microsoft" in Microsoft's trademarked font at the top of the message, which represents to the user that the message is from Microsoft's MSN. Figure 5 below is an image of this email.

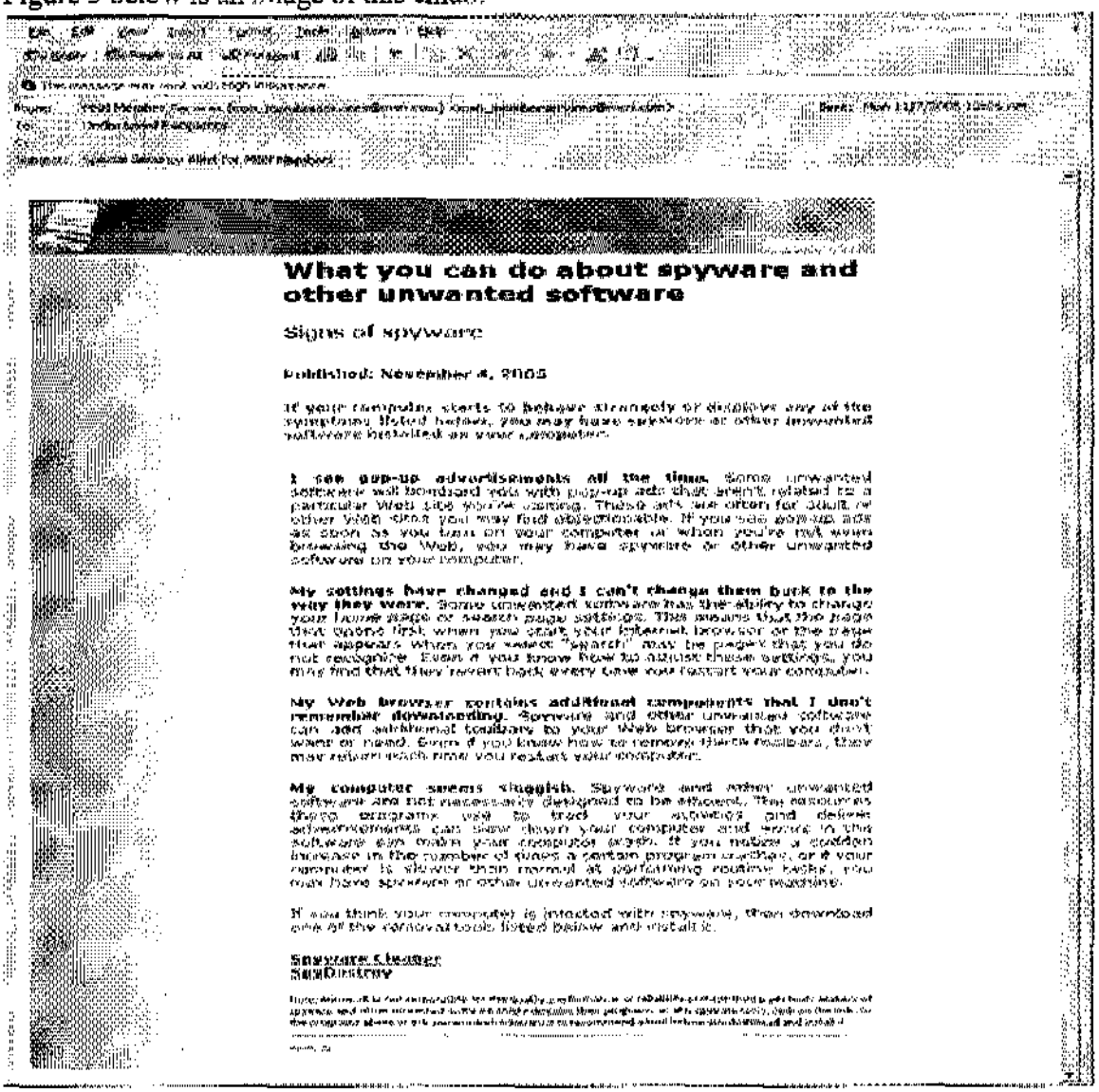


Figure 5.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

One version of the email message includes a footer claiming that the message is copyrighted by Microsoft and include two hyperlinks to actual Microsoft Web sites, along with a link to Spyware Cleaner earlier in the email. The implied representation that the product Spyware Cleaner is recommended by Microsoft increases the likelihood that a consumer will purchase the product. In fact, neither the message nor the product has an affiliation with Microsoft.

9.9 The practices described above constitute unfair and deceptive acts or practices in trade or commerce and unfair methods of competition in violation of the Consumer Protection Act, RCW 19.86.020.

D. Fifteenth Cause of Action: Misrepresentations – Defendant Traub

9.10 Plaintiff realleges paragraphs 1.1 through 9.9 and incorporates them herein as if set forth in full.

9.11 In the context of his advertising, promotion, and marketing of Spyware Cleaner, Traub represents that the software is a Microsoft anti-spyware product. In fact, Spyware Cleaner is not affiliated in any way with Microsoft. Traub advertises and has advertised Spyware Cleaner using Google's AdWords, an advertising program through Google.com, a well-known search engine. Traub advertises Spyware Cleaner in the form of a hyperlink titled: "Microsoft AntiSpyware." The hyperlink advertisement appears when a user types one of the following search terms into the Google search box: "Microsoft spyware cleaner," "Microsoft antispyware," or "Microsoft anti-spyware." When the user clicks on the hyperlink advertisement, the user is redirected to www.myspywarecleaner.com, the Web site for Spyware Cleaner. Spyware Cleaner is not affiliated in any way with Microsoft's anti-spyware software. Defendant's advertisement has the capacity to deceive viewers into believing that Spyware Cleaner is a Microsoft product or is being promoted, recommended, or sanctioned by Microsoft. For each sale of Spyware Cleaner generated by his advertisement, Defendant receives a commission of 75% of the purchase price. Figure 6 below depicts a typical search

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

that produces a link, which, if clicked on, will take the user to SCL's Web site for Spyware Cleaner. The second hyperlink entitled "**Microsoft** AntiSpyware" in the "sponsored links" box on the left side of the page is Traub's advertisement.

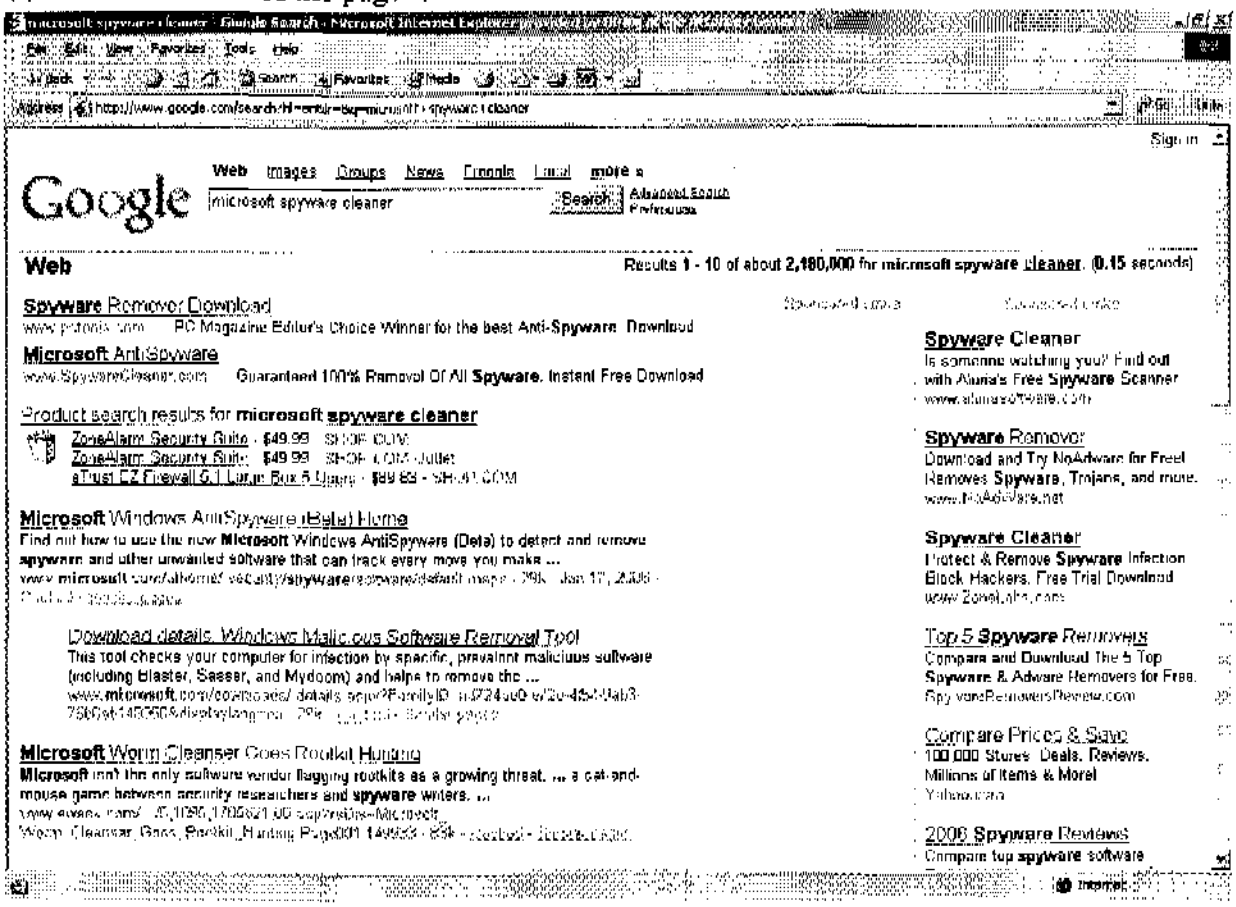


Figure 6.

9.12 The activities described above constitute unfair and deceptive acts or practices in trade or commerce and an unfair method of competition in violation of the Consumer Protection Act, RCW 19.86.020.

E. Sixteenth Cause of Action: Deceptive Tampering With Operating System Hosts File – Defendants SCL, Burke, and Preston

9.13 Plaintiff realleges paragraphs 1.1 through 9.12 and incorporates them herein as if set forth in full.

9.14 During the installation process of the free scan software, without the user's knowledge or consent, Defendants' program deletes the user's Hosts file, which is a file in which the user could place Web site addresses or other code indicating to the computer not to go to those sites or not to permit a certain function. In effect, the Hosts file is a security file for the user.

9.15 The activity described above constitutes an unfair and deceptive act or practice in trade or commerce and an unfair method of competition in violation of the Consumer Protection Act, RCW 19.86.020.

F. Seventeenth Cause of Action: False Detection of Spyware – Defendants SCL, Burke, and Preston

9.16 Plaintiff realleges paragraphs 1.1 through 9.15 and incorporates them herein as if set forth in full.

9.17 After Defendants' "free scan" of the user's computer is complete, a new browser window automatically opens, taking the user to Defendants' Web site, www.myspywarecleaner.com, where the results of the scan are displayed. The scan always detects something that it labels as spyware, when, in fact, what it labels as spyware is usually a cookie or harmless registry key, or simply not installed on the computer at all. For example, numerous scans on different computers, the results showed 17 "BonzaiBuddy" registry keys, which were labeled as spyware; however, Bonzai Buddy software was not, in fact, installed on any of the computers that were scanned.

9.18 The activity described above constitutes an unfair and deceptive act or practice in trade or commerce and an unfair method of competition in violation of the Consumer Protection Act, RCW 19.86.020.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

G. Fifteenth Cause of Action: False Spyware Removal – SCL, Burke, and Preston

9.19 Plaintiff realleges paragraphs 1.1 through 9.18 and incorporates them herein as if set forth in full.

9.20 Beneath the report indicating all of the supposedly dangerous files detected on the user's computer is a button stating "Click to Remove Infections." When the user clicks on the button, the user is told via a dialogue box that they need to register the product, indicating that there is a full version of the anti-spyware software. The message urges the computer user to remove the infections quickly. When the user clicks to register, the user is taken to www.myspywarecleaner.com in a new browser window, where the user can purchase Spyware Cleaner.

9.21 After purchasing Spyware Cleaner, the user receives a registration code by email. The user enters the registration code on the Spyware Cleaner Web site. At that point, if the user performs another scan, the program again detects the same allegedly harmful registry keys. When the user clicks to remove the infections, the programs performs a function and then reveals that there are no more infections on the computer.

9.22 In fact, Defendants' alleged "removal" of "infections" on the user's computer constitutes a misrepresentation. The "infections" that are "detected" in the original scan of the computer are not, in fact, "infections." If they even exist as files, they are cookies or harmless registry keys. Their "removal" is not the removal of "infections." Furthermore, by representing to the user that the "removal" function has been successfully executed, Defendants create the illusion that their software has effectively removed spyware that was previously on the user's computer. Consumers who may, in fact, have real, pernicious spyware on their computers continue to have it, while believing that Defendants' software has eradicated it.

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

9.24 The activity described above constitutes an unfair and deceptive act or practice in trade or commerce and an unfair method of competition in violation of the Consumer Protection Act, RCW 19.86.020.

H. Sixteenth Cause of Action: Deceptive and Misleading Pop-Up Advertisements – SCI., Burke, and Preston

9.25 Plaintiff realleges paragraphs 1.1 through 9.24 and incorporates them herein as if set forth in full.

9.26 Defendants disseminate, and cause to be disseminated, advertisements for Spyware Cleaner on hundreds of Web sites. Defendants' advertisements appear in the form of a grey dialogue box with a blue border, similar to the dialogue boxes utilized by the Microsoft Windows operating system when sending security-related messages. The text of the advertisements warns the user that their computer may be infected with harmful spyware and that immediate removal may be necessary, and offers the user a free scan to determine if their computer is infected. If the user does not want a free scan and clicks on the button "no," the Spyware Cleaner Web site nevertheless opens in a new browser window on the user's machine. By automatically opening a new browser window with the Spyware Cleaner Web site loaded, Defendants' advertisements deceptively force the user to continue to view more advertisements for Spyware Cleaner. In addition, by simulating buttons on their advertisements that normally permit a user to close a pop-up or cancel an action, Defendants deceptively force the user to continue to view more advertisements for Spyware Cleaner.

9.27 Defendants further deceive computer users regarding the nature of their advertisements by trapping the user in a succession of "warning" messages. After the user is taken to the Spyware Cleaner Web site, if the user clicks on the "x" in the upper right-hand corner to close the new browser window, another pop-up advertisement appears on the user's computer. This pop-up also appears as a grey box with a blue border resembling a Microsoft

Windows security dialogue box. The pop-up again warns that the user's computer may be infected with dangerous spyware and that immediate removal may be necessary. The user again is offered a free scan to determine whether their computer is infected. The user is then given the option of clicking on "next" – in order to get the free scan – or "cancel," presumably to close the pop-up. However, the "cancel" button does not work. If the user clicks anywhere in the entire pop-up except for on the "x", yet another pop-up will appear, warning the user again about harmful spyware and offering a free scan of their computer.

9.28 The activity described above constitutes an unfair and deceptive act or practice in trade or commerce and an unfair method of competition in violation of the Consumer Protection Act, RCW 19.86.020.

X. THIS COURT'S POWER TO GRANT RELIEF

10.1 The CAN-SPAM Act empowers this Court to enjoin further violations by defendants. 15 U.S.C. § 7706(f)(1)(A). This Court is also empowered to award the greater of actual or statutory damages. 15 U.S.C. § 7706(f)(1)(B).

10.2 The Commercial Electronic Mail Act, RCW 19.190, may be enforced by this Court through pendant jurisdiction. 28 U.S.C. § 1367. This Court is empowered to award the greater of actual or statutory damages under the Act. RCW 19.190.040(1).

10.3 The Computer Spyware Act, RCW 19.270, may be enforced by this Court through pendant jurisdiction. 28 U.S.C. § 1367. This Court is empowered to enjoin further violations of the Act and to award the greater of actual or statutory damages under the Act. RCW19.270.060.

10.4 The Consumer Protection Act, RCW 19.86, may be enforced by this Court through pendant jurisdiction. 28 U.S.C. § 1367. This Court is empowered to grant injunctive and such other relief as it may deem appropriate to halt and redress violations of the Consumer Protection Act, including civil penalties and costs and fees. RCW 19.86.080, 19.86.090.

XI. PRAYER FOR RELIEF

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

11.1. WHEREFORE, Plaintiff, STATE OF WASHINGTON, prays that this Court grant the following relief:

a. Adjudge and decree that Defendants have engaged in the conduct complained of herein;

b. Adjudge and decree that the conduct complained of in paragraphs 6.2 through 6.27 constitutes violations of the CAN-SPAM Act, 15 U.S.C. § 7701, et seq;

c. Adjudge and decree that the conduct complained of in paragraphs 7.2 through 7.6 constitutes violations of the Commercial Electronic Mail Act, RCW 19.190, and pursuant to RCW 19.190.030(3), constitutes per se violations of the Consumer Protection Act, RCW 19.86, et seq.;

d. Adjudge and decree that the conduct complained of in paragraphs 8.2 though 8.21 constitutes violations of the Computer Spyware Act, RCW 19.270, et seq;

e. Adjudge and decree that the conduct complained of in paragraphs 9.2 though 9.28 constitutes unfair or deceptive acts or practices in violation of the Consumer Protection Act, RCW 19.86;

f. Permanently enjoin Defendants and their representatives, successors, assigns, officers, agents, servants, employees, and all other persons acting or claiming to act for, on behalf of, or in active concert or participation with Defendants from continuing or engaging in the unlawful conduct complained of herein;

g. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the CAN-SPAM Act, the Commercial Electronic Mail Act, the Computer Spyware Act, and the Consumer Protection Act;

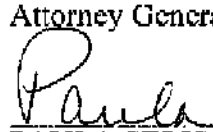
h. Assess a civil penalty, pursuant to RCW 19.86.140, of up to $2,000 for each violation of RCW 19.86.020 caused by the conduct herein;

ATTORNEY GENERAL OF WASHINGTON
Consumer Protection Division
900 Fourth Avenue, Suite 2000
Seattle, WA 98164-1012
(206) 464-7744

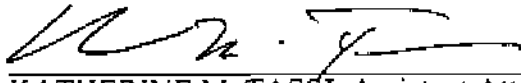
i. Award Plaintiff the costs of bringing this action, pursuant to 15 U.S.C. § 7706(f)(4), RCW 19.86.090, and 19.270.060, as well as such other and additional relief as the Court may determine to be just and proper.

DATED this 24th day of January, 2006.

Presented by:
ROB MCKENNA
Attorney General



PAULA SELIS, Senior Counsel
WSBA #12823
Office of the Attorney General of Washington
900 Fourth Avenue, Suite 2000
Seattle, Washington 98164-1012
Phone: 206.464.7744
Facsimile: 206.587.5636
paulas@atg.wa.gov



KATHERINE M. TASSI, Assistant Attorney General
WSBA #32908
Office of the Attorney General of Washington
900 Fourth Avenue, Suite 2000
Seattle, Washington 98164-1012
Phone: 206.464.7744
Facsimile: 206.587.5636
katherinet@atg.wa.gov

Attorneys for Plaintiff
State of Washington