

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE**

FEDERAL TRADE COMMISSION,

Plaintiff,

Civil No.

v.

SEISMIC ENTERTAINMENT
PRODUCTIONS, INC.,
SMARTBOT.NET, INC., and
SANFORD WALLACE,

COMPLAINT FOR INJUNCTION
AND OTHER EQUITABLE RELIEF

Defendants.

Plaintiff, the Federal Trade Commission (“FTC” or “Commission”), for its Complaint alleges as follows:

1. The Commission brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), to obtain preliminary and permanent injunctive relief, restitution, disgorgement and other equitable relief against the Defendants for their unfair acts or practices in connection with their marketing and their distribution of software programs to consumers in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over this matter pursuant to 15 U.S.C. §§ 45(a), 52, and 53(b); and 28 U.S.C. §§ 1331, 1337(a) and 1345.

3. Venue in the United States District Court for the District of New Hampshire is proper under 15 U.S.C. § 53(b), as amended by the FTC Act Amendments of 1994, Pub. L. No. 103-312, 108 Stat. 1691,

and 28 U.S.C. §§ 1391(b) and (c).

PLAINTIFF

4. Plaintiff, the Federal Trade Commission, is an independent agency of the United States government created by statute. 15 U.S.C. §§ 41 *et seq.* The Commission enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The Commission is authorized to initiate federal district court proceedings by its own attorneys to enjoin violations of the FTC Act and to secure such equitable relief as may be appropriate in each case, including restitution for injured consumers, consumer redress, and disgorgement. 15 U.S.C. § 53(b).

DEFENDANTS

5. Defendant Seismic Entertainment Productions, Inc. (“Seismic”) is a New Hampshire corporation with its principal place of business located at 11 Farmington Road, Rochester, New Hampshire 03867. Since at least December 2003, and continuing thereafter, Seismic has marketed various products, including purported “anti-spyware” software called “Spy Wiper” and “Spy Deleter,” on behalf of others. Seismic advertises these products through “pop-up” advertisements displayed to consumers using various Internet web sites that it controls, including the web sites at www.default-homepage-network.com and downloads.default-homepage-network.com. Seismic also downloads to and installs on consumers’ computers various advertising and other software programs, including Favoriteman, TrojanDownloader and Clearsearch. Seismic transacts or has transacted business in the District of New Hampshire.

6. Defendant SmartBot.Net, Inc. (“SmartBot”) is a Pennsylvania corporation with its corporate

address at 3 Cobblestone Court, Richboro, Pennsylvania 18954, and its principal place of business at 495 Route 9, Barrington, New Hampshire 03825. Since at least December 2003, and continuing thereafter, SmartBot has marketed various products, including purported “anti-spyware” software called “Spy Wiper” and “Spy Deleter,” on behalf of others. SmartBot advertises these products through pop-up advertisements displayed to consumers using various Internet web sites that it controls, including the web sites at www.passthison.com, object.passthison.com, and www.smartbotpro.net. In addition, the pop-up advertisements served by SmartBot also are displayed when a computer user visits various Internet web sites controlled by Seismic, including, but not limited to, www.default-homepage-network.com. SmartBot transacts or has transacted business in the District of New Hampshire.

7. Defendant Sanford Wallace (“Wallace”) is or has been President and owner of Defendants Seismic and SmartBot at all times material to this Complaint. Acting individually or in concert with others, Wallace has formulated, directed, controlled, or participated in the acts and practices of Seismic and SmartBot, including the acts and practices complained of below. Wallace resides and/or transacts or has transacted business in the District of New Hampshire.

8. Collectively, Defendants Seismic, SmartBot, and Wallace have operated and continue to operate a common enterprise while engaging in the unfair acts and practices alleged below, and are therefore jointly and severally liable for said acts and practices.

COMMERCE

9. The acts and practices of Seismic, SmartBot, and Wallace (collectively, “Defendants”) alleged in this Complaint are or have been in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. §§ 44.

DEFENDANTS’ BUSINESS PRACTICES

Introduction

10. Since at least November 2003, Defendants, in numerous instances, have exploited particular vulnerabilities in certain versions of the Microsoft Internet Explorer web browser (“IE web browser”) to reconfigure consumers’ computers by installing software code onto their computers without their knowledge or authorization. The software code, among other things, (a) changes the IE web browser’s home page; (b) modifies the IE web browser’s search engine; and (c) downloads and installs various advertising and other software programs, including, but not limited to, Favoriteman, TrojanDownloader, Clearsearch, WinFetcher, 7Search.com, and VX2; and (d) causes an incessant stream of pop-up advertisements to be displayed.

11. A web browser, which is used by a computer to locate and view Internet web pages, serves as a liaison between a computer and the information delivered to the computer through the Internet. Most web browsers, including the IE web browser, generate a notification message to the user whenever software code is being downloaded to the user’s computer from the Internet. The notification message gives the user the option to authorize or not authorize the download. By exploiting certain vulnerabilities in the IE web browsers, however, Defendants have been able to download and install software code without triggering the display of the IE web browser notification message. In the absence

of such notification message, consumers neither knew of nor authorized the software downloads and installations.

12. Defendants control or have controlled a network of Internet web sites, including, but not limited to, www.default-homepage-network.com, downloads.default-homepage-network.com, www.passthison.com, object.passthison.com, and www.smartbotpro.net, through which they send or have sent to consumers' computers the software code exploiting vulnerabilities in the IE web browser. Defendants use or have used various means to direct consumers' computers to these web sites. In some instances, Seismic and Wallace use or have used online advertising networks to disseminate banner advertisements on various third-party Internet web sites, including, but not limited to, the web sites at www.kingsofchaos.com and www.cdmsports.com. Unsuspecting consumers who visit or have visited these web sites at the time defendants' ads are displayed are automatically sent to one of Defendants' web sites.

13. Once consumers' computers are redirected to, or otherwise visit, Defendants' web sites, the software code Defendants download and install causes a cascade of pop-up advertisements, including full-page advertisements, to be displayed on consumers' computers and causes a number of advertising and other software programs to be downloaded to and installed on consumers' computers. In numerous instances, Defendants' practices cause or have caused consumers' computers to malfunction, slow down, crash, or cease working properly, and cause or have caused consumers to lose data stored on their computers.

Unauthorized Changes to Consumers' Internet Web browsers

14. Through the use of the web sites and pop-up advertisements referred to above, Defendants

download and install or have downloaded and installed, without consumers' knowledge or authorization, certain software code, which replaces the IE web browser home page on consumers' computers with different web pages that have been and are controlled by Seismic and Wallace, including, the web page at <http://default-homepage-network.com/start.cgi?hk1m>. When consumers open or have opened their IE web browsers, they are or have been sent to web pages that Seismic and Wallace control or have controlled. At these web pages, Defendants launch or have launched a series of pop-up advertisements, including full-page advertisements, and web pages. In many instances, these pop-up advertisements and web pages prevent and have prevented consumers from accessing their intended Internet web sites. Affected consumers are or have been compelled to exit the IE web browser and reinitiate their Internet connections in an effort to regain control over their IE web browser. This process often is or has been repeated multiple times, even after consumers have returned the IE web browser to its original home page, because through the series of pop-up advertisements and web pages, Defendants continuously download and have downloaded software code to consumers' computers that modifies the browser.

15. Defendants, through the use of the web sites and pop-up advertisements referred to above, also download or install or have downloaded and installed, without consumers' knowledge or authorization, certain other software code that replaces the IE web browser search engine with a different search engine, including a search engine known as 7Search.com. After such software code is installed, when consumers first activate the search function of their IE web browser's search engine, the different search engine is launched and subsequent Internet searches are rerouted to this new search engine. By hijacking these Internet searches, the new search engine controls the results that are sent to consumers' computers, including any hyperlinks or pop-up advertisements.

Unauthorized Downloads of Software programs

16. Defendants, through the use of the web sites and pop-up advertisements referred to above, download and install or have downloaded to and installed on, without consumers' knowledge or authorization, various advertising and other software programs to consumers' computers. Defendants download or have downloaded some of these software programs, including TrojanDownloader, WinFetcher and Clearsearch, from the web site downloads.default-homepage-network.com. This web site is or has been controlled by Seismic and Wallace. The software code that Defendants use to exploit a vulnerability in the IE web browser, which triggers the download and installation of these programs to consumers' computers, is or has been downloaded from the web site object.passthison.com. This web site is or has been controlled by SmartBot and Wallace. Among other things, the TrojanDownloader, WinFetcher, and Clearsearch software programs disseminate pop-up advertisements, hijack Internet searches, and create security holes that are used to download and install more advertising and other software programs without consumers' knowledge or authorization, including the software program known as VX2. The security holes establish a connection between consumers' computers and an Internet server, through which information can be downloaded to the computer from the server and uploaded from the computer to the server, without consumers' knowledge or authorization.

17. Defendants also download or have downloaded to consumers' computers additional software programs residing on the web sites and Internet servers of others. For example, Defendants download or have downloaded the software program Favoriteman to computers from the third-party web site www.addictivetechologies.net. The software code that Defendants use to exploit a vulnerability in the IE web browser, which triggers the download and installation of Favoriteman, also is or has been

downloaded from the www.addictivetechologies.net web site. Favoriteman creates a security hole on consumers' computers that is used to download and install more software programs, including, but not limited to, VX2, Ezula, and ShopatHome.com, without consumers' knowledge or authorization. Among other things, these additional software programs track web pages visited by consumers, monitor information consumers enter into online forms, and survey Internet searches conducted by consumers.

Defendants' Dissemination of Online Advertisements

18. Among the pop-up advertisements Defendants disseminate or have disseminated through the means described above are advertisements that market Spy Wiper and Spy Deleter, purported "anti-spyware" software, both of which are sold for \$30. See Exhibits 1, 2, and 3. One advertisement mimics the "Notepad" feature of the IE web browser and displays a message stating:

If your NOTEPAD launched and is displaying this message. . . Then 'Spyware' programmers can control applications on YOUR computer and it is URGENT that you download SPY WIPER immediately. Do not allow spyware programs to damage your insecure computer!! (See other window).

[Exhibit 1, as of August 30, 2004]

A separate advertisement causes the computer's CD-ROM tray to open and states:

FINAL WARNING !!

If your cd-rom drive(s) open . . .

You **DESPERATELY NEED** to rid your system of spyware pop-ups
IMMEDIATELY!

Spyware programmers can control your computer hardware if you failed to protect your computer right at this moment!

Download Spy Wiper NOW!

[Exhibit 2, as of August 30, 2004]

Finally, a third advertisement promoting Spy Deleter displays a large stop-sign and states:

IMPORTANT SECURITY NOTICE FROM SPY DELETER!

Is your computer suffering from the any of the following symptoms:

- 1. Has your browser's **START PAGE** changed?
- or 2. Are you seeing a recent increase in annoying **POP UPS**?
- or 3. Have **PORN** ads appeared in your browser or email?
- or 4. Has your computer been acting weird lately?
- or 5. Is your Internet **slower** or even crashing?
- or 6. Do you think your computer may have a virus?
- or 7. Have new programs or toolbars been added **without your permission**?

If your computer is experiencing any of these symptoms . . .

It is almost certain that “**spyware**” has taken over your computer, and the problems will **only get worse quickly**. Plus your sensitive information like **credit cards and all your passwords** can be retrieved by **criminals all around the world**. This is a very scary problem that needs immediate attention! You **NEED to get this fixed now!**

Click on **THIS LINK FOR IMMEDIATE HELP** and your computer will be back to normal and secure again in just a few minutes.

[Exhibit 3, emphasis in original, as of August 30, 2004]

Defendants Ill-Gotten Revenues

19. Defendants generate or have generated substantial revenues through exploiting the vulnerability in the IE web browser to modify the IE web browser and to download and install advertising and other software programs on behalf of others. Parties such as Defendants often receive or have received a commission on sales made through advertisements that they have disseminated to consumers and

receive fees from software vendors based on the number of software downloads and installs that they have induced.

COUNT ONE

Unfairly Changing Consumers' Web Browsers

20. In numerous instances, through the means described in Paragraphs 10 through 15, Defendants download and install or have downloaded and installed software code onto consumers' computers that makes substantial modifications to these computers' IE web browser without consumers' knowledge or authorization. Among other things, such software code changes (a) the IE web browser home page to a different web page controlled by Defendants; and (b) the IE web browser search engine to a different search engine.

21. As a result of these changes, consumers have received a stream of pop-up advertisements, have had their Internet searches hijacked, have had their web browsers redirected to Defendants' own web pages, and have had their computers' memory and other resources depleted. For many consumers, Defendants' practices have caused their computers to malfunction, lose important information, operate more slowly, and in some cases, cease working completely.

22. Consumers are required to spend substantial time and money to resolve these problems with their computers. Consumers can not reasonably avoid this substantial injury because Defendants have exploited a vulnerability in their computers' IE web browsers to download and install without their knowledge or authorization the software code that leads to the injury. Defendants' practices do not benefit consumers or competition. Thus, Defendants practices cause or are likely to cause substantial injury that cannot be reasonably avoided, and this injury is not outweighed by countervailing benefits to

consumers or competition.

23. Therefore, Defendants' practices, as described in Paragraphs 20 through 22 above, are unfair and violate Section 5 of the FTC Act, 15 U.S.C. § 45(a).

COUNT TWO

Unfairly Installing Advertising and Other Software Programs

24. In numerous instances, through the means described in Paragraphs 10 through 17, including making significant modifications to computers' IE web browsers, Defendants download and install or have downloaded and installed software code onto consumers' computers without their knowledge or authorization. In turn, this software code downloads and installs advertising and other software programs.

25. These software programs display a stream of pop-advertisements, create security holes through which other software programs and malicious code can be downloaded, hijack Internet searches for information, and deplete the computers' memory and other resources. For many consumers, Defendants' practices have caused their computers to malfunction, lose important information, operate more slowly, and in some cases, cease working completely.

26. Consumers are required to spend substantial time and money to resolve these problems with their computers. Consumers can not reasonably avoid this substantial injury because Defendants have exploited a vulnerability in their computers' IE web browsers to download and install without their knowledge or authorization the software code that leads to the injury. Defendants' practices do not benefit consumers or competition. Thus, Defendants practices cause or are likely to cause substantial injury that cannot be reasonably avoided, and this injury is not outweighed by countervailing benefits to

consumers or competition.

27. Therefore, Defendants' practices, as described in Paragraph 24 through 26 above, are unfair and violate Section 5 of the FTC Act, 15 U.S.C. § 45(a).

COUNT THREE

Unfairly Compelling Purchase of "Anti-Spyware" Software

28. In numerous instances, through the means described in Paragraphs 10 through 18, to induce consumers to purchase "anti-spyware" software products, Defendants download and install or have downloaded and installed software code on computers that affects their functionality. In particular, the software code has changed the IE web browser home page on consumers' computers, has replaced the IE web browser's search engine, has displayed fake IE web browser notepad pages, and has caused the computers' CD-ROM trays to eject. The Defendants then have disseminated to consumers experiencing these functionality problems a stream of pop-up advertisements, including advertisements that promote "anti-spyware" software called "Spy Wiper" or "Spy Deleter." The Defendants' advertisements for Spy Wiper or Spy Deleter, including, but not limited to, Exhibits 1 through 3, warn consumers that they must purchase the advertised products immediately to resolve the specific computer problems that Defendants themselves have caused. As described above in Paragraph 19, Defendants have profited when consumers have purchased the Spy Wiper and Spy Deleter software as a result of Defendants' acts and practices.

29. Defendants' course of conduct in marketing the Spy Wiper and Spy Deleter software has compelled consumers to either spend \$30 to purchase the advertised software, or otherwise spend substantial time and money to resolve these problems with their computers. Consumers can not

reasonably avoid this substantial injury because Defendants have exploited a vulnerability in their computers' IE web browsers to download and install without their knowledge and authorization the software code that negatively affects their computers' functionality. Defendants' course of conduct has no benefits to consumers or competition. Thus, Defendants practices cause or are likely to cause substantial injury that cannot be reasonably avoided, and this injury is not outweighed by countervailing benefits to consumers or competition.

30. Therefore, defendants' practices, as described in Paragraphs 28 through 29 above, are unfair and violate Section 5 of the FTC Act, 15 U.S.C. § 45(a).

CONSUMER INJURY

31. Defendants' violations of Section 5 of the FTC Act, 15 U.S.C. § 45(a), as set forth above, have caused and continue to cause substantial injury to consumers. Absent injunctive relief by this Court, defendants are likely to continue to injure consumers and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

32. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and other ancillary relief, including consumer redress, disgorgement and restitution, to prevent and remedy any violations of any provision of law enforced by the Federal Trade Commission.

PRAYER FOR RELIEF

WHEREFORE, plaintiff, the Federal Trade Commission, requests that this Court, as authorized by Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and pursuant to its own equitable powers:

1. Award plaintiff such preliminary injunctive and ancillary relief as may be necessary to avert the likelihood of consumer injury during the pendency of this action and to preserve the possibility of

effective final relief.

2. Permanently enjoin the Defendants from violating Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), as alleged in this Complaint.
3. Award such equitable relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act, including, but not limited to, rescission of contracts and restitution, and the disgorgement of ill-gotten gains;
4. Award Plaintiff the costs of bringing this action as well as such additional equitable relief as the Court may determine to be just and proper.

Dated: October 6, 2004

Respectfully submitted:

/s/ T. David Plourde

T. David Plourde No. 2044
U.S. Attorney's Office
55 Pleasant Street
Concord, NH 03301
(603) 225-1552/1470 (voice/fax)
david.plourde@usdoj.gov

FOR THE FEDERAL TRADE COMMISSION:

WILLIAM E. KOVACIC

General Counsel

/s/ Laura M. Sullivan

Laura M. Sullivan (New York Bar No.2919660)
Charulata Pagar (Illinois Bar No. 6209680)
Federal Trade Commission
601 New Jersey Avenue, N.W.
Washington, D.C. 20001
(202) 326-3327/2791 (Offices)
(202) 326-3259 (Fax)

Attorneys for Plaintiff