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,

Defendants.

MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION FOR A TEMPORARY RESTRAINING ORDER WITH EXPEDITED DISCOVERY, PRESERVATION OF DOCUMENTS AND ORDER TO SHOW CAUSE WHY A PRELIMINARY INJUNCTION SHOULD NOT ISSUE AGAINST DEFENDANTS

I. INTRODUCTION

The Federal Trade Commission ("FTC" or "Commission") brings this action to halt defendants' Internet marketing scheme that has seized control of consumers' computers nationwide, infected them with spyware and other malicious software programs, bombarded them with pop-up advertisements, and exposed them to unnecessary computer security risks in violation of Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a). Defendants' unlawful activity already has injured hundreds of consumers, thwarting their ability to use the Internet and their computers, and, in many cases, causing their computers to malfunction, slow down, cease working properly, or even crash. In addition, after infecting consumers' computers, defendants offer to sell them an "anti-spyware" product that purportedly can fix their computers and stop the pop-up ads – that is, selling consumers a solution to the problems they created.

Consumers using the Internet easily fall victim to defendants' scheme. Defendants hijack computers while consumers are surfing the Internet and direct them to visit one of defendants' web sites. In some cases, defendants use pop-up ads, which are placed on a wide range of third-party web sites, to hijack computers. Unsuspecting consumers who visit these third-party web sites at the time one of defendants' ads are being displayed are automatically sent to defendants'

II. JURISDICTION AND VENUE

This court has subject matter jurisdiction over the FTC's claims pursuant to 15 U.S.C. § § 45(a) and 53(b) and 28 U.S.C. § § 1331, 1337(a) and 1345. Venue in this District is proper pursuant to 15 U.S.C. § 53(b) and 28 U.S.C. 1391(b) - (c). Sanford Wallace and the corporate defendants are located in New Hampshire, and all transact or have transacted business in New Hampshire.

III. PARTIES

A. Plaintiff

The FTC is an independent agency of the United States government created by the FTC Act, 15 U.S.C. § § 41-58. The Commission is charged, among other things, with enforcement of 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. Section 13(b) of the FTC Act, 15. U.S.C. § 53(b), authorizes

President of Seismic, and runs both their operations. *See* PX 2, S. Schools (FTC Investigator) Dec. Atts. K - M and O.

Wiper, defendants receive 45% of the $30 purchase price (*i.e.*, $13.50) for each spyware removal product that they induce consumers to buy. *See, e.g.*, PX 2, S. Schools Dec. ¶ 53 & Att. R.

IV. DEFENDANTS' UNFAIR BUSINESS PRACTICES

A. Defendants Trick Computers to Visit Their Network of Web Sites.

Defendants use their network of web sites to download spyware to computers that visit them. Defendants employ various means to direct computers to visit their obscure web sites. In at least some cases, defendants disseminate Internet ads that automatically redirect computers to their web sites. *See* PX 3, A. Bluman (24/7 Real Media, Inc.) Dec. ¶ 8 & Att. C. Defendants have used Internet advertising networks to disseminate banner ads to third-party web sites. *See* PX 3, A. Bluman (24/7 Real Media, Inc.) Dec. ¶ 11 & Att. E, Att. I; PX 4, B. Gelb (Kings of Chaos) Dec. ¶ 13 & Att. C. Internet advertising networks are companies that place ads on web sites participating in their ad network for a fee to the advertiser, and compensate these "publisher" web sites for the ad placement. *See* A. Bluman (24/7 Real Media, Inc.) Dec. ¶ 2; PX 4, B. Gelb (Kings of Chaos) Dec. ¶ 3. Defendants have submitted to the Internet advertising networks ads containing software code that automatically sends computers to one of their web sites, including the web site www.default-homepage-network.com. *See, e.g.*, PX 3, A. Bluman (24/7 Real Media, Inc.) Dec. ¶ 8 & Att. C; PX 8, J.C. Kennedy Dec. ¶ ¶ 2-5; PX 14, J. White Dec. ¶ 2. Computers of unsuspecting consumers who visit third-party web sites at the time they are displaying one of defendants' ads are redirected to a web site operated by the defendants. This redirection occurs without consumers clicking on anything on their computer screen or otherwise signaling their consent to visit a different web site. *See, e.g.*, PX 14, J. White Dec. ¶ 2; PX 3, A. Bluman (24/7 Real Media, Inc.) Dec. ¶ 16 & Att. H. *See also* PX 9, P. Mancine Dec. ¶ 5.

B. Defendants Exploit a Vulnerability in Certain Versions of the IE Explorer to Download Spyware to Consumers' Computers.

Once consumers' computers are redirected to, or otherwise visit, defendants' web site www.default-homepage-network.com, defendants exploit a security vulnerability in recent versions of the IE web browser to download spyware. *See* Expert Declaration of Steven D. Gribble, Ph.D.(PX 1) ¶ ¶ 9, 22-26, 36, 38 & Att. F (Microsoft Corporation, Inc. Affidavit).[1] A web browser is a software application that runs on a computer, and is used to navigate the Internet. In response to commands it receives from the computer user, the web browser locates web pages and displays them on the computer. A web site with which the browser establishes a connection can send information, including spyware or other "bad" software code, to the computer. *See* PX 1 ¶ ¶ 17, 20-21. Basically, the web browser functions as a gatekeeper, sitting between the Internet and the computer, and screens "good" and "bad" web content. Defendants therefore can gain access to the computer by tricking the web browser to accept spyware. *See* PX 1 ¶ ¶ 9, 15, 22, 36, 38 & Att. F.

More than 75 percent of computers currently use the IE web browser to navigate the Internet. *See* PX 1 ¶ 23. The IE web browser offers multiple security levels to users – low, medium, high, and customized. *See* PX 1 ¶ 24 & Att. F. The security level controls how the IE web browser responds to attempts by web sites to download software code to the computer. The IE web browser's default security level, which is used by most computer users, is "medium." *See id*. A web browser set to the medium security level is supposed to generate a notification

[1]The FTC provides the expert declaration of Dr. Stephen D. Gribble, Ph.D. Dr. Gribble is an assistant professor in the Computer Science Department at the University of Washington. He has documented and evaluated the effects on computers of visiting defendants' network of web sites.

message to the computer user each time a web site attempts to download software code to the computer. *See* PX 1 ¶ 9, 22-25 & Att. F. This notification message provides the computer user with the option to authorize or not authorize the download. *See id.*

Defendants exploit a known vulnerability in versions 5.01, 5.5, and 6.0 of the IE web browser to download their spyware to computers without triggering the display of the IE web browser notification message to the user. *See* PX 1 ¶ 7-9, 15, 35-36, 38 & Att. F. Defendants' spyware contains software code that instructs the IE web browser, even when set at the default security level, to "trust" the spyware program and download it automatically to the computer. *See id*

[2]The experience in part is shown in a video file appended to PX 2 (S. Schools Dec.) as Attachment A, which captures the series of events occurring on a computer screen after the computer is infected with defendants' spyware.

IP Addresses, and DNS Names) and PX 2, S. Schools Dec. ¶ ¶ 36, 41, 43 & Atts. D-G, K-L. Upon visiting this web page, the computer screen is peppered with a cascade of pop-up advertisements, including ads that cover the entire screen and promote adult entertainment web sites. *See* PX 1 ¶ ¶ 7, 15, 33-38; PX 2, S. Schools Dec. ¶ ¶ 4-30 & Att. A; PX 5, A. Buehring Dec. ¶ 3, 6 & Atts. A-D; PX 9, P. Mancine Dec. ¶ ¶ 3, 6 & Att. A; PX 11, M. Murphy Dec. ¶ 2; PX 13, J. VanDenburgh Dec. ¶ 3. Many of these pop-up ads are sent from the web sites www.passthison.com, server224smartbotpro.net, and object.passthison.com., which are controlled by defendants. *See* PX 1 ¶ ¶ 33-36 & Att. B and PX 2, S. Schools Dec. ¶ ¶ 36, 42-43 & Atts. F, G and L. The web site also automatically directs the computer to visit other web pages and launches windows on the computer screen. *See* PX 1 ¶ ¶ 34-36. These pop-up ads, launched windows, and web pages that prevent users from accessing their intended web sites. *See* PX 2. *See also, e.g.*, PX 8, J.C. Kennedy Dec. ¶ 8; PX 9 P. Mancine Dec. ¶ ¶ PX 12, B. Pansano Dec. ¶ ¶ 4-8; PX 13, J. VanDenburgh Dec. ¶ 3.

In addition, the spyware replaces the IE web browser's search engine with a different search engine. *See* PX 1. In at least some cases, the new search engine is 7Search.com. *See* PX 1 ¶ ¶ 6, 36(b). The new search engine is immediately launched at the time the computer user attempts to conduct a search on the IE web browser's default search engine. The new search engine overrides the search functions of the IE web browser's default search engine. *See* PX 1

Þ X

"trojan horse" programs. *See* PX 1 ¶ 38; PX 5, A. Beuhring Dec. ¶ 6; PX 9, P. Mancine Dec. ¶ 8. The trojan horse programs establish a beachhead on the computer and are used to install more software. *See* PX 1 ¶ ¶ 37(d), 38(b), 39. The trojan horse programs also could be used to infect it with viruses, worms, and more trojans, or even to steal credit card and other financial information stored on it. *See* PX 1 ¶ 39. The programs that the spyware installs include, among others, Favoriteman, TrojanDownloader, WinFetcher, VX2, and Clearsearch.[3] *See* PX 1 ¶ 37(d), 38(b). These programs bombard computers with even more pop-up ads, monitor where users travel on the Internet, hijack Internet searches, insert tool bars on web pages, collect information entered into online forms, and create security holes that are used to install even more software. *See* PX 1 ¶ ¶ 37(d), 38(b), 39.

Infected computers are caught in a trap. Users whose computers are infected with the spyware are forced to end their Internet sessions and reinitiate them in an effort to regain control of their computers. *See, e.g.,* PX 9, P. Mancine Dec. ¶ 4; PX 11, M. Murphy Dec. ¶ 6; PX 12, B. Pansano Dec. ¶ 8. *See also* PX 1 ¶ ¶ 7, 10, 12. Because defendants' spyware changes the default home page to one of their web pages, upon re-opening the IE web browser, the computer returns to www.default-homepage-network.com and the spyware is downloaded yet again. *See* PX 1 ¶ 7, 10, 12. Consumers who re-set the IE web browser to its original default home page setting are also trapped. These consumers are often forced to repeat the home page re-setting process

[3]Favoriteman and TrojanDownloader are software programs that establish a beachhead on the computer, which they use to install additional advertising and other software programs. *See* PX 1 and PX 2, S. Schools Dec. Atts. T-U. VX2 monitors Internet activity and collects information computer users enter into online forms. *See* PX 2, S. Schools Dec. Att. V. Clearsearch installs a web search tool bar and hijacks computer users' search requests. *See* PX 2, S. Schools Dec. Att. W. WinFetcher is another advertising program that tracks where users go on the Internet. *See* PX 2, S. Schools Dec. Att. X. VX2, Clearsearch, and WinFetch all send targeted pop-up ads based on information they collect. *See* PX 2, S. Schools Dec. Atts. V-X.

multiple times because the spyware changing the web browser's default home page to one of defendants' web pages is continually reinstalled to their computers. *See* PX 1 ¶ ¶ 7, 10, 12; *See also, e.g.,* PX 10, K. Matto Dec. ¶ ¶ 4-8; PX 11, M. Murphy Dec. ¶ ¶ 5-6; PX 12, B. Pansano Dec. ¶ 8.

D. Defendants Disseminate Pop-Up Ads for "Anti-Spyware" Products to the Same Computers They Have Infected With Spyware.

The defendants' web sites disseminate to the computers they infect with spyware pop-up ads marketing "anti-spyware" products called either Spy Deleter or Spy Wiper. *See* PX 1 ¶ ¶ 13, 34(a), 37(a) & Atts. D and G; PX 5, A. Beuhring Dec. ¶ 4 & Att. A; PX 9, P. Mancine Dec. ¶ ¶ 3, 5, 8 & Att. A. The ads for Spy Deleter or Spy Wiper generally claim that affected computers are likely infected with spyware, and that Spy Deleter or Spy Wiper can resolve any problems that these computers may be experiencing because of it. *See id*. For example, one pop-up ad shows a large red 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!**

[4]Notepad is a basic text editor software program that is used to create text documents.

sales commission on all sales that they generated. *See* PX 2, S. Schools Dec. ¶ 53 & Att. R

E. Defendants' Practices Have Caused Widespread and Substantial Injury to Consumers.

Defendants' spyware has caused widespread and substantial injury to consumers. These consumers include school districts, libraries, businesses, and individual computer users throughout the United States. *See* PX 2, S. Schools Dec. ¶ 45, PX 3 - PX 14. More than 300 consumers have filed complaints with the FTC, which likely represents a small percentage of the total number of consumers that defendants' practices have injured and continue to injure. *See* PX 2, S. Schools Dec. ¶ 45. *See also* PX 1 ¶ 14. These consumers complain that their default home pages have been changed to different web pages, their computers are bombarded with pop-up ads, including ads that promote Spy Deleter or Spy Wiper and adult entertainment services, and that they can no longer use the Internet. *See, e.g.*, PX 5, A. Beuhring Dec. ¶ ¶ 3,4; (default

PX 7, R. Kaur, ¶ ¶ 3-5; PX 8, J. C. Kennedy Dec. ¶ 8; PX 12, B. Pansano Dec. ¶ 8; PX 14, J. White Dec. ¶ 6. *See also* PX 1 ¶ 15. As a result, computer users have lost important data and their productivity at work has been significantly reduced. *See, e.g.*, PX 5, A. Beuhring Dec. ¶ 3, 7; PX 8, J. C. Kennedy Dec. ¶ 11; PX 13, J. VanDenburgh Dec. ¶ 8.

It is a complicated undertaking for consumers to fix their computers after they are infected with defendants' spyware. *See* PX 1 ¶ 15. Consumers are required to spend substantial time or money in this task. *tly reduced.*

the Internet, software code that exploits security vulnerabilities in the IE web brower or any other web browser to install spyware and that makes unauthorized changes to the IE web browser or any other browser; (2) requiring that the defendants remove the software code that exploits the IE web browser from any web site or web page under their control; (3) requiring that the defendants preserve business and financial records concerning their Internet marketing activities and produce or make available certain documents; (4) requiring that the defendants provide an accounting, including completed financial forms; (5) granting limited expedited discovery; and (6) requiring that the defendants show cause, if there is any, why this Court should not enter a preliminary injunction, pending final ruling on the Complaint. This relief is authorized by Section 13(b) of the FTC Act in conjunction with Fed. R. Civ. P. 65, and is necessary and appropriate in this case.

"Section 13(b) of the [FTC Act] authorizes

[5]*See also FTC v. Amy Travel Serv., Inc.*, 875 F.2d 564, 572 (7th Cir. 1989) ("under Section 13(b), the statutory grant of authority to the district court to issue permanent injunctions includes the power to order any ancillary equitable relief necessary to effectuate the exercise of the granted powers.").

district court may order broad, equitable, preliminary relief that is necessary to make permanent relief possible, especially where, as here, the public interest is at stake. *See Porter v. Warner Publishing Holding* Co., 328 U.S. 395, 398 (1946) ("since the public interest is involved in a proceeding of this nature, [the court's] equitable powers assume an even broader and more flexible character than when only a private controversy is at stake."); *Gem Merchandising*, 87 F.3d at 469 ("absent a clear command to the contrary, the district court's equitable powers are extensive"); *FTC v. Direct Marketing Concepts, Inc.* 2004 WL 1399185, slip op. (D. Mass. June 23, 2004) (court issued preliminary injunction with asset restrictions and granted FTC right of immediate access to defendants' business premises).[6]

B. This Case Meets the Standard for the Issuance of a TRO and a Preliminary Injunction.

The Commission meets its burden of proof for issuance of a TRO and preliminary injunction.[7] Section 13(b) of the FTC Act allows a district court to grant the FTC a preliminary injunction "[u]pon a proper showing that, weighing the equities and considering the [FTC's] likelihood of ultimate success, such action would be in the public interest." 15 U.S.C. § 53(b). *See also Stillwater Vending*, No. 97-386-JD, slip op. at 1-2 (Ex. A). To obtain an injunction, the FTC must show: (1) there is a substantial likelihood it will prevail on the merits; (2) on balance,

---

[6]*See also FTC v. Patriot Alcohol Testers,* Inc., No. 91-11812-C, 1992 WL 27334 *3 (D. Mass. 1992) ("the Court is authorized to issue preliminary injunction as well as an order freezing assets when the attendant facts and circumstances so warrant as an exercise of its broad equitable powers"); *FTC v. Dion*, Civ. No. 03-40005-NMG, slip op. at 4 (D. Mass. 2003) (converting previously issued TRO with asset freeze into preliminary injunction) (copy attached as Exhibit B).

[7]The FTC is seeking a noticed TRO, and therefore the same standards should apply for both the TRO and preliminary injunction. *See* 9 Wright & Miller, Federal Practice & Procedure § 2951 (1995).

[8]The FTC is not required to meet the traditional four-part standard for issuance of an injunction. Although the FTC does not bear the burden of establishing irreparable harm, *see FTC v. Patriot Alcohol Testers,* Inc., No. 91-11812-C, 1992 WL 27334 *3 (D. Mass. 1992), *citing FTC v. Rare Coin Galleries of America, Inc.* 1986-2 Trade Cas. (CCH) ¶ 67, 338 at 61, 473 (D. Mass. 1986), without the relief requested in the proposed TRO order, there is a substantial risk that the public will suffer injury that is "serious and permanent." *Planned Parenthood League of Massachusetts v. Bellotti*, 641 F. 2d. 1006, 1023 (1st Cir. 1981). *See also*

computers will lose data, malfunction, slow down to a crawl, cease to work properly, or even crash. *See, e.g.*, PX 5, A. Beuhring Dec. ¶ 3; PX 7, R. Kaur Dec. ¶ ¶ 3, 9; PX 9, P. Mancine Dec. ¶ 3; PX 10, K. Matto, ¶ ¶ 3, 5, 8; PX 11, M. Murphy Dec. ¶ ¶ 2-6; PX 13, J. VanDenburgh ¶¶ 3, 5-6.

Although many consumers suffered substantial harm as a result of defendants' practices, it is also well-settled that "[i]njury may be sufficiently substantial if it causes a small harm to a large class of people." *J.K. Pubs. Inc.*, 99 F. Supp. 2d 1176, 1201. *See also FTC v. Pantron Corp.*, 33 F.3d 1088, 1102 (9th Cir. 1994) ("[C]onsumer injury is substantial when it is the aggregate of many small individual injuries."); *FTC v. Crescent Publ'g Group, Inc.*, 129 F. Supp. 2d 311, 322 (S.D.N.Y. 2001) (finding that "injury to consumers was substantial in the aggregate"). In this case, consumers whose computers are infected with defendants' spyware are forced to spend time or money to fix them. *See* PX 1 ¶ 15 and *e.g.*, PX 5, A. Beuhring Dec. ¶ 7; PX 7, R. Kaur Dec. ¶ 10; PX 9, P. Mancine Dec. ¶ 6; PX 12, B. Pansano, ¶ 12; PX 13, J.Vandenberg Dec. ¶ 8. Although the degree of injury to each consumer varies depending on factors such as the length of time it takes to locate and remove the spyware, their computers' memory resources and operating systems, the purposes for which they use their computers, and their level of technological knowledge, in the aggregate, the injury consumers have suffered is substantial. *See id.* Defendants' spyware has affected consumers across the United States, including schools, businesses, libraries, and scores of individuals who rely on the Internet. PX2, S. Schools Dec. ¶ 45; PX3 - PX14. In each case, their use of the Internet and their computers has been compromised, and they had to take substantial steps to remedy it. PX2, S. Schools Dec. ¶ 45; PX3 - PX14.

Defendants also engage in practices that compel some consumers to pay $30 for "anti-spyware" products. Defendants infect consumers' computers with spyware and then offer them a means to remove it – Spy Deleter or Spy Wiper. Defendants' ads for Spy Deleter or Spy Wiper warn consumers that their computers are likely infected with spyware, and that a whole litany of harms will result, such as "spyware programmers controll[ing] [their] computers" and criminals stealing their "sensitive information like credit cards and all [their] passwords." *See* Complaint Ex. 3; *see also* Complaint Ex. 1. In an effort to regain control of their computers, in some cases, consumers are compelled to purchase Spy Deleter or Spy Wiper, and thus defendants' practices hinder consumers' ability to make "free-market" choices about purchasing anti-spyware or other computer security products. *See, e.g.,* PX 6, C. Gordon Dec. ¶ 4; PX 7, R. Kaur Dec. ¶ 10; s*ee also* FTC Unfairness Policy Statement, Ex. C, at p. 4 & fn. 22; *Arthur Murray Studio, Inc. v. FTC*, 458 F.2d 622 (5

consequences for consumers that are not accompanied by an increase in services or benefits" to them or the market as a whole, the unfairness standard is clearly met. *See Windward Mktg.*, 1997 U.S. Dist. LEXIS 17114, *32. The evidence shows that consumers' lose control of their computers and the Internet, and in exchange receive only a deluge of pop-up ads and spyware. Thus, defendants practices provide no benefit to consumers or competition.

c. Consumers Cannot Reasonably Avoid the Injury Caused by Defendants' Practices

The test for unavoidable injury depends upon "whether consumers had a free and informed choice that would have enabled them to avoid the unfair practice." *Windward Mktg.*, 1997 U.S. Dist. LEXIS 17114, at *32. *See also J.K. Publications*, 99 F. Supp. 2d at 1201. The evidence demonstrates that consumers do not have a "free or informed choice" in becoming infected with defendants' spyware. Defendants use security vulnerabilities in the IE web browser to download spyware to consumers' computers without generating the standard notification message to the computer screen. *See* PX 1 ¶ ¶ 9, 15, 36, 38 & Att. F. Consumers do not receive this message even when they have tried to protect their computers by using the medium security setting for their IE web browser, and even using additional security products such as firewalls or anti-virus programs. *See id.*; PX 7; *see also* R. Kaur Dec. ¶ 6; PX 10, K. Matto Dec. ¶ 11. Without the display of this IE web browser notification message, however, consumers are denied the choice to accept or reject defendants' downloading of spyware to their computers, and have no knowledge that it even occurs. Therefore, consumers cannot reasonably

The defendants operate as a common enterprise and, therefore are jointly and severally liable for their violations of the FTC Act. *See F.T.C. v Think Achievement Corp.* 144 F.Supp. 2d. 992, 1011 (N.D. Iowa Sept. 29, 2000). Courts have recognized the Commission's right to treat multiple defendants as a single economic entity. *See id.*; *Sunshine Art Studios, Inc. v. FTC*, 481 F.2d 1171, 1173 (1st Cir. 1973). Factors considered in determining whether defendants operate a common enterprise are: (1) common ownership and control; (2) shared office space and offices; (3) business is transacted through a maze of interrelated companies; and (4) funds are commingled. *See F.T.C. v. Think Achievement Corp*. 144 F. Supp. Supp. 2d. at 1011. The corporate defendants Seismic and SmartBot share the same owner, officer and director – Mr. Wallace – operate out of the same location, intermingle funds, and work closely together to distribute spyware. *See* PX 2, S.Schools Dec. ¶ ¶ 36, 41, 43 & Atts. D-G, Atts. K-L, Atts. M-P; *see also* PX 1 ¶ ¶ 30-38 & Att. C.

Mr. Wallace personally pays for Seismic's and SmartBot's business expenses. *See* PX 2, S.Schools Dec. ¶ ¶ 43, 43 & Atts. K-L. In addition, SmartBot's billing address is Mr. Wallace's current home address in Barrington, New Hampshire. *See* PX 2, S.Schools Dec. ¶ 43 & Att. L. The web sites of both companies operate together to effectuate the illegal marketing scheme. For example, Seismic's web sites automatically take visitors to SmartBot's web sites. *See* PX 1 ¶ 33-38 & Att. C. SmartBot's web sites download to consumers' computers spyware that changes their IE web browser home web pages to a web page that is registered to Seismic. One of Seismic's web sites delivers the pop-up ad that markets the "anti-spyware" products Spy Deleter or Spy Wiper. *ee* PX 1 ¶ 37. Defendants act as a single economic entity, which Mr. Wallace controls, and share the common goal of making money by distributing spyware to

consumers' computers through a complicated network of web sites.

The FTC also is likely to succeed in establishing that defendant Mr. Wallace is individually liable for the corporate practices. Courts have held an individual defendant personally liable for restitution if: "(1) the corporate defendants violated the FTC Act; (2) [he] participated directly in the wrongful acts or pr

[11]*See also FTC v. Publishing Clearing House, Inc.*, 104 F.3d 1168, 1170 (Defendant's "assumption of the role of president . . . and her authority to sign documents on behalf of the corporation demonstrate that she has the requisite control over the corporation."); *Windward Mktg.*, 1997 U.S. LEXIS 17114, at *38 ("An individual's status as a corporate officer gives rise to a presumption of ability to control a small, closely-held corporation.")

[12]For example, Mr. Wallace has paid for at least some of Seismic's bills for its web sites from his personal bank account. *See* PX 2, S. Schools Dec. ¶ 41, & Att. K. He also instructed the company hosting one of SmartBot's web sites to send invoices for the web site to his home address in Barrington, NH. *See* PX 2, S. Schools Dec. ¶ 43, & Att. L.

knowledge."[13] *Amy Travel*, 875 F.2d at 574. To satisfy the knowledge requirement, it is sufficient to show an individual was aware of the wrongful conduct and failed to use his authority to control the corporate defendants to correct it.[14] *See Windward Mktg.*, 1997 U.S. LEXIS 17114, at *39-40.[15] Mr. Wallace had requisite knowledge to be held individually liable for the corporate defendants' violations of the FTC Act. He has played an active role in running his companies; the primary goal of which has been to make money through infecting consumers' computers with spyware and then offering them a means to remove it.

2. The Balance of Hardships Favors the Issuance of an Injunction

The public interest advanced by the FTC far outweighs any limited interest the Defendants' may have in continuing to download spyware to consumers' computers without their knowledge or authorization. In balancing the hardships to the public interest against a private interest, "the public interest should receive greater weight." *FTC v. World Wide Factors Ltd.*, 882 F.2d 344, 347 (9th Cir. 1989). *See also Standard & Poor's Corp., Inc. v. Commodity Exch., Inc.*, 683 F.2d 704, 711 (2d Cir. 1982). The public equities to consider include, but are

---

[13]Intent to commit illegal acts is not necessary to obtain injunctive relief against an individual. *See Five-Star Auto Club, Inc.*, 97 F. Supp. 2d *502*, 535 (S.D.N.Y. 2000). *See also Amy Travel*, 875 F.2d at 574; *Publishing Clearing House*, 104 F.3d at 1171.

[14]The knowledge element can be satisfied by showing: (1) the individual had actual knowledge of the illegal conduct; (2) was recklessly indifferent to whether the conduct was illegal; or (3) had an awareness of a high probability that the conduct was illegal, along with an intentional avoidance of the truth. *See Publishing Clearing House, Inc.*, 104 F.3d at 1171.

[15]*See also Gem Merchandising*, 87 F.3d at 470 ("having found [defendant] had direct control over the activities of Gem Merchandising, and that he was aware of the illegal practices, the court properly held [him] individually liable"). In fact, defendants posted on their web sites a message acknowledging that their practices were problematic, and claiming that they would cease this summer. *See* PX 2, S. Schools Dec. ¶ 31 & Atts. B-C. However, contrary to their statements, their wrongful practices have continued. *See* PX 2, S.Schools Dec. ¶ 32; PX 1 ¶ 14.

unnecessary security risks.[17] Defendants' practices prevent consumers from using their computers and the Internet. Affected computers, in many cases, malfunction, slow down, cease working properly, or even crash, and consumers may lose important data stored on them. Defendants' practices cause consumers to lose precious time and money fixing their computers that are infected with spyware, adware, and other unwanted programs. In some cases, consumers are compelled to spend money purchasing purported "anti-spyware" products that defendants market and from which defendants profit. Defendants' practices interfere with a broad swath of consumers – businesses, schools, libraries, and countless consumers nationwide have fallen victim to their home page hijacking scheme. *See* PX 2, S.Schools Dec. ¶ 45; PX 3- PX 14. In short, it is strongly in the public interest to end defendant's injurious practices immediately.

C. A TRO Order Requiring Defendants' to Remove the Dangerous Code from Their Web Sites and Servers and to Preserve Documents and Granting the FTC Expedited Discovery Is Necessary to Preserve Effective Final Relief

This Court has broad equitable authority under Section 13(b) of FTC Act to grant ancillary relief necessary to accomplish complete justice. *See, e.g., Amy Travel Serv., Inc.*, 875 F.2d 564, 571-72; *FTC v. H.N. Singer, Inc.*, 668 F.2d 1107, 1113 (9th Cir. 1982); *Five-Star Auto Club, Inc.*, 97 F. Supp. 2d at 533. An order requiring Defendants to remove the dangerous software code from web sites and web pages under their control is necessary to stop consumer harm. Given their past pattern of conduct and the revenues at stake, requiring defendants to

[17]Even if defendants immediately cease the challenge practices and therefore argue that a temporary or preliminary relief is not warranted, injunctive relief is still appropriate where, as here, there is a risk that the harm will recur. *See United States v. W.T. Grant Co.*, 345 U.S. 629, 633 (1953) ("Along with its power to hear the case, the court's power to grant injunctive relief survives discontinuance of the illegal conduct. . . . The purpose of an injunction is to prevent future violations") (*citations omitted*). As long as defendants' web sites publish software code that can exploit security vulnerabilities in the IE web browser, their practices can easily be resuscitated. *See* PX 1 ¶ 14.

remove the software code that exploits the IE web browser from their web sites and web pages is wholly within the court's equitable powers and will protect consumers from injury during the pendency of the litigation. *See SEC v. R.J. Allen & Assoc., Inc.*, 386 F. Supp. 866, 877 (S.D. Fla. 1974) (past conduct "gives rise to inference that there is a reasonable likelihood of future violations.").

As part of the final recovery in the case, the FTC will seek to redress injured consumers and disgorge the full amount of defendants' unjust enrichment from their illegal practices.[18] An order requiring Defendants to retain records and conduct an accounting, and allowing for expedited discovery, will preserve the possibility of redress for victimized consumers and accurate disgorgement of defendants' ill-gotten gains. An accounting of defendants' assets and an order preserving documents is necessary to identify defendants' assets, calculate the amount of defendants' proceeds from their illegal marketing activities, and to fully determine the size and extent of the injuries.[19] Although at this juncture the FTC does not seek an asset freeze or restriction, to maintain the status quo and preserve the potential for a monetary remedy, we request an order requiring defendants' to provide an accounting and to retain their business and financial records. *See FTC v. Direct Marketing Concepts, Inc.* 2004 WL 1399185, slip op. (D.

---

[18]The FTC routinely obtains consumer redress, including disgorgement, when courts find that defendants violated the FTC Act. *See, e.g.*, *FTC v. Gem Merchandising Corp.*, 87 F.3d 466, 470 (held that disgorgement was appropriate to "deprive wrong-doer of his ill-gotten gain" collected through illegal telemarketing practices) (citation omitted); *See also FTC v. Pantron I Corp*, 33 F.3d 1088, 1103 (9th Cir. 1994) (ordering payment of monetary relief to the extent of defendant's unjust enrichment from false advertising claims). *See also FTC v. Mylan Laboratories, Inc.*, 62 F.Supp. 2d. 25, 37 (D.D.C. 1999) (upholding FTC's authority to seek disgorgement as a remedy in district court).

[19]The FTC is concerned that Mr. Wallace will dissipate his assets. For example, in May 2004, New York-New York Hotel & Casino and Mirage Casino obtained a judgment of $425,096.40 against Mr. Wallace for unpaid debts. *See* PX 2, S.Schools Dec. ¶ 51.

Mass. June 23, 2004) (court ordered asset restrictions and accounting); *FTC v. Patriot Alcohol Testers,* Inc., No. 91-11812-C, 1992 WL 27334 *3 (D. Mass. 1992) (court issued asset freeze); *FTC v. Dion*, Civ. No. 03-40005-NMG, slip op. at 4 (D. Mass. 2003) (TRO order with asset freeze converted to preliminary injunction) (Ex. B). *See also SEC v Fife*, 311 F.2d 1 (1st Cir, 2002) (affirmed order freezing defendants' assets).

Finally, the FTC seeks immediate production of or access to certain documents related to defendants' business practices and expedited discovery that is narrow in scope to quickly and efficiently identify: (1) web sites and Internet servers that may be distributing the software exploit code and the Internet service providers (ISPs) hosting these web sites and servers;[20] (2) possible additional defendants; (3) documents and records pertaining to defendants' businesses, including electronic records; (4) defendants' assets and proceeds from the challenged practices; (5) third-parties that paid defendants affiliate marketing fees;[21] and (6) extent of the injury that the challenged practices have caused. *See FTC v. Direct Marketing Concepts, Inc.* 2004 WL 1399185 (court ordered expedited discovery and immediate access to premises). The Federal Rules of Procedure 26(d), 33(a), and 34(b) authorize this Court to depart from the standard discovery provisions, including the applicable time frames88 02.od0ovees 108 tnlicable time fn sTT

[20]The FTC seeks the identities of the ISPs hosting defendants' web sites in part because, in the event the Court grants the requested TRO order, this information will allow us to immediately notify them and better monitor defendants' compliance with the order's injunctive provisions.

[21]Upon discovering information sufficient to identify the affiliates who potentially benefitted from defendants' illegal practices, the FTC will notify them of the pending litigation and seek documents and information relevant to defendants' business practices and profit-taking, as well as locating potential victims.

and their operations are constantly changing. Without the swift collection of documents and

600 Pennsylvania Avenue, NW,
NJ-3212
Washington, DC 20580
(202) 326-3327/2791 (voice)
(202) 326-3259 (fax)