

**SUPREME COURT OF THE STATE OF NEW YORK  
COUNTY OF NEW YORK**

-----X  
**THE PEOPLE OF THE STATE OF NEW YORK**  
by **ELIOT SPITZER, Attorney General**  
of the State of New York,

**Petitioners,**

**-against-**

**DIRECTREVENUE, LLC, and**  
**JOSHUA ABRAM, ALAN MURRAY, DANIEL**  
**KAUFMAN and RODNEY HOOK, individually,**

**Respondents.**  
-----X

**AFFIRMATION OF**  
**JUSTIN BROOKMAN**

**Index No. \_\_\_\_\_**

JUSTIN BROOKMAN, an attorney admitted to practice before the Courts of the State of New York, makes the following affirmation under the penalty of perjury.

1. I am an Assistant Attorney General in the office of ELIOT SPITZER, Attorney General of the State of New York, assigned to the Internet Bureau. I am familiar with the facts and circumstances of this proceeding.

2. The facts set forth in this affirmation are based upon information contained in the files of the Internet Bureau.

3. I submit this affirmation in support of the Attorney General's application for an Order which, inter alia, (a) enjoins respondents' violation of New York General Business Law §§ 349-50, Executive Law § 63(12) and New York common law; (b) requires respondents to issue an accounting and (c) requires respondents to pay disgorgement of profits, revenue and/or unjust enrichment, as appropriate, and penalties and costs to the State of New York.

**A. Parties**

4. **Petitioners** are the people of the State of New York, by **their attorney**, Eliot Spitzer, Attorney General of the State of New York. **Petitioners** have **offices** in the County of New York, located at 120 Broadway, New York, New York.

5. **Respondent DirectRevenue, LLC** (“**Direct Revenue**”) is a Delaware corporation with its principal place of business at 107 **Grand Street, New York, New York**. See Exh. 1 (**Direct Revenue** privacy policy). Since the company’s **founding** in 2002, **Direct Revenue** has been **responsible for the distribution of over 150 million spyware programs to computer users all over the world**. See Exh. 2 (**Direct Revenue** response to interrogatories) at 1-2 & Schedule 2. In many (if not all) cases, **Direct Revenue** has installed these programs **without giving disclosure to the users, and without obtaining the users’ consent**.

6. **Respondent Joshua Abram** is **Direct Revenue’s** Executive Vice President for **Business Development**. See Exh. 3 (listing of **Direct Revenue** management team). **Prior to taking this post** in mid-2005, Abram served as **Chief Executive Officer** of the company. **Along with respondents Murray, Kaufman and Hook, Abram founded Direct Revenue** in November 2002. See Exh. 4 (Limited Liability Company Agreement for **Direct Revenue, LLC**). Since that time, Abram has been **aware of, participated in and directed Direct Revenue’s deceptive spyware practices**. Abram is a resident of New York.

7. **Respondent Alan Murray** is the **Chief Product Officer** for **Direct Revenue**. See Exh. 3. Until **August 2005**, he served as the company’s **Chief Operations Officer**. Murray was **one of the four founders** of **Direct Revenue** in November 2002. See Exh. 4. **Since that time, Murray has been aware of, participated in and directed Direct Revenue’s deceptive spyware**

practices. Murray is a resident of New York.

8. Respondent Daniel Kaufman is Direct Revenue's Executive Vice President for Corporate Development. See Exh. 3. Kaufman was one of the four founders of Direct Revenue in November 2002. See Exh. 4. Since that time, Kaufman has been aware of, participated in and directed Direct Revenue's deceptive spyware practices. Kaufman is a resident of New York.

9. Respondent Rodney Hook is Direct Revenue's Chief Technology Officer. See Exh. 3. Prior to August 2005, Hook's position with the company was Chief Scientist. Hook was one of the four founders of Direct Revenue in November 2002. See Exh. 4. Since that time, Hook has been aware of, participated in and directed Direct Revenue's deceptive spyware practices.

**B. Direct Revenue's Deceptive Spyware Installations: Background**

**Background: How Direct Revenue Distributes its Spyware Without User Consent**

10. Since 2002, the respondents have created a lucrative business by surreptitiously installing intrusive computer programs onto millions of computers worldwide. The programs, designed by Direct Revenue and known alternatively as "spyware," "adware" or "malware," serve a perpetual stream of pop-up advertisements from Direct Revenue's clients to users surfing the internet. In selecting which pop-up ads to show, the programs also monitor the websites visited by infected users, along with data typed into web forms (such as search engines or online questionnaires). Among the names Direct Revenue has given these programs are "Aurora," "Ceres," "Best Offers," "OfferOptimizer" and "VX2."

11. The pop-up ads generated by Direct Revenue spyware are intrusive and annoying, as they perpetually interrupt users' internet browsing experiences with ads for products such as

online gambling, car and home refinancing, and “adult” dating services. Respondents have designed their programs to inundate users’ screens with so many ads that, in the words of Direct Revenue’s top executives, they “hammer” and “abuse” those who have the software.

12. Annoying though they may be, these programs might be permissible had users consented to having them installed onto their computers. But the Attorney General’s extensive investigation shows that Direct Revenue installs its spyware onto users’ hard drives without informing the users, and without obtaining their consent.

13. In most cases, Direct Revenue (or distributors hired by Direct Revenue) have advertised to consumers free programs, such as screensavers or games. When the consumer agrees to download an advertised free program, a small code is placed on the consumer’s computer which then instructs Direct Revenue’s servers to silently install Direct Revenue spyware as well. Spyware commentators commonly call this practice “bundling,” and refer to the free programs that sneak the spyware onto users’ computers as “trojan horses.”

14. In twenty-nine separate tests conducted by this office of twenty-one different websites, Direct Revenue installed spyware onto our test computers without providing reasonable or conspicuous notice. To the extent that any notice was provided at all, it was generally hidden in a long, legalistic “license agreement” or “terms of service” for the advertised free program – which no ordinary consumer would be likely to read. Certainly, no ordinary consumer would suspect that such a license agreement would contain notice of an unrelated, sophisticated spyware program.

15. In some cases, Direct Revenue and its distributors have exploited vulnerabilities in Microsoft’s operating system and web browser to simply unilaterally install their own software

from websites without notice that any software is being downloaded. This tactic is commonly known as a “drive-by download,” because it provides no clue to even savvy web users that something – anything – is being placed on their computers. Investigators from this office detected Direct Revenue’s spyware being installed in just this manner from multiple websites, including websites featuring hardcore child pornography.

16. Direct Revenue has long been aware that its hidden or non-existent notice practices leave consumers with no idea how, when or where they were infected with its spyware. As one internal Direct Revenue email succinctly concluded, “99% of users believe ad software was maliciously installed without their consent” See Exh. 5 (email from R. Minassian to D. Doman dated June 15, 2005) (attaching sampling of representative complaints).

**Background: Direct Revenue Spyware  
Evades Detection and Removal and Installs Other Spyware**

17. Like a resistant disease, Direct Revenue designs its software to be extremely difficult to eliminate from a hard drive. First, it places its spyware in unlikely locations on a user’s hard drive, often with randomly generated names and modification dates. Until recently, Direct Revenue also configured its spyware to avoid appearing in Microsoft’s “Add/Remove Programs” utility – the most common mechanism by which users remove software from their computers.

18. Worse, Direct Revenue designs its spyware to resist efforts to manually delete it, or to delete it using common anti-virus or anti-spyware software. Many times, the spyware even reinstalls itself after removal.

19. Direct Revenue’s spyware also allows the company permanent remote access to

all infected computers. Using this backdoor, Direct Revenue has persistently “updated” its spyware programs to add increasingly sophisticated versions of its pop-up programs. It has also used this backdoor to silently install still more spyware programs, such as third-party pop-up programs, and programs that silently redirect users to Direct Revenue websites.

20. Joshua Abram, Alan Murray, Daniel Kaufman and Rodney Hook (collectively the “individual respondents”) founded Direct Revenue in November 2002, and have directed and overseen its operations ever since. As numerous emails cited infra demonstrate, each of the individual respondents has actively encouraged and profited from the deceptive practices outlined above and herein, during the past three years.

**C. Direct Revenue’s Deceptive “Bundling” of Spyware with Other Software**

21. Between November 2004 and September 2005, the Office of the Attorney General (“OAG”) conducted tests of all websites we were able to locate that distributed Direct Revenue’s spyware programs, twenty-one in all. In those tests, OAG investigators documented Direct Revenue’s spyware installing itself onto undercover test computers without meaningful (if any) notice or disclosure, and without user consent. With limited exception, notice about bundled Direct Revenue spyware programs was provided either not at all, or in a lengthy End User License Agreement (“EULA”) or “terms of service” that users never saw unless they (a) clicked on a vaguely worded link to “terms and conditions,” and then (b) set aside considerable time to wade through countless pages of legal jargon.

22. Such deceptive practices are not merely part of Direct Revenue’s business model; they are the entire basis of its business model. In fact, during our year-long investigation, virtually every website we tested that distributed Direct Revenue’s spyware failed to provide

conspicuous notice of the spyware installed.<sup>1</sup>

23. The following pages (pp. 7-37) describe the tests the OAG conducted of the sites used by Direct Revenue to distribute its spyware programs. For greater detail with regard to each of these downloads, please refer to the accompanying Affidavits of Vanessa Ip ("Ip Aff."), Joseph Rivela ("Rivela Aff.") and Sibü Thomas ("Thomas Aff.").

Deceptive Installation from FasterXP.com

24. Direct Revenue installs much of its spyware by hiring third parties to bundle Direct Revenue spyware along with their own software programs. Although these third-party installations are initiated by Direct Revenue's distributors (and any subdistributors hired by those distributors), Direct Revenue's servers actually install the spyware. Direct Revenue's distributors and subdistributors merely install a small code onto an infected computer that calls back to Direct Revenue to download and install the spyware. See Exh. 6 (letter from N. Klausner to K. Dreifach et al. dated January 17, 2006). Thus, even in those instances where Direct Revenue has hired third parties to distribute its spyware, Direct Revenue's computer servers have actually delivered and installed the hidden spyware programs without notice to, or consent from, the computer user.

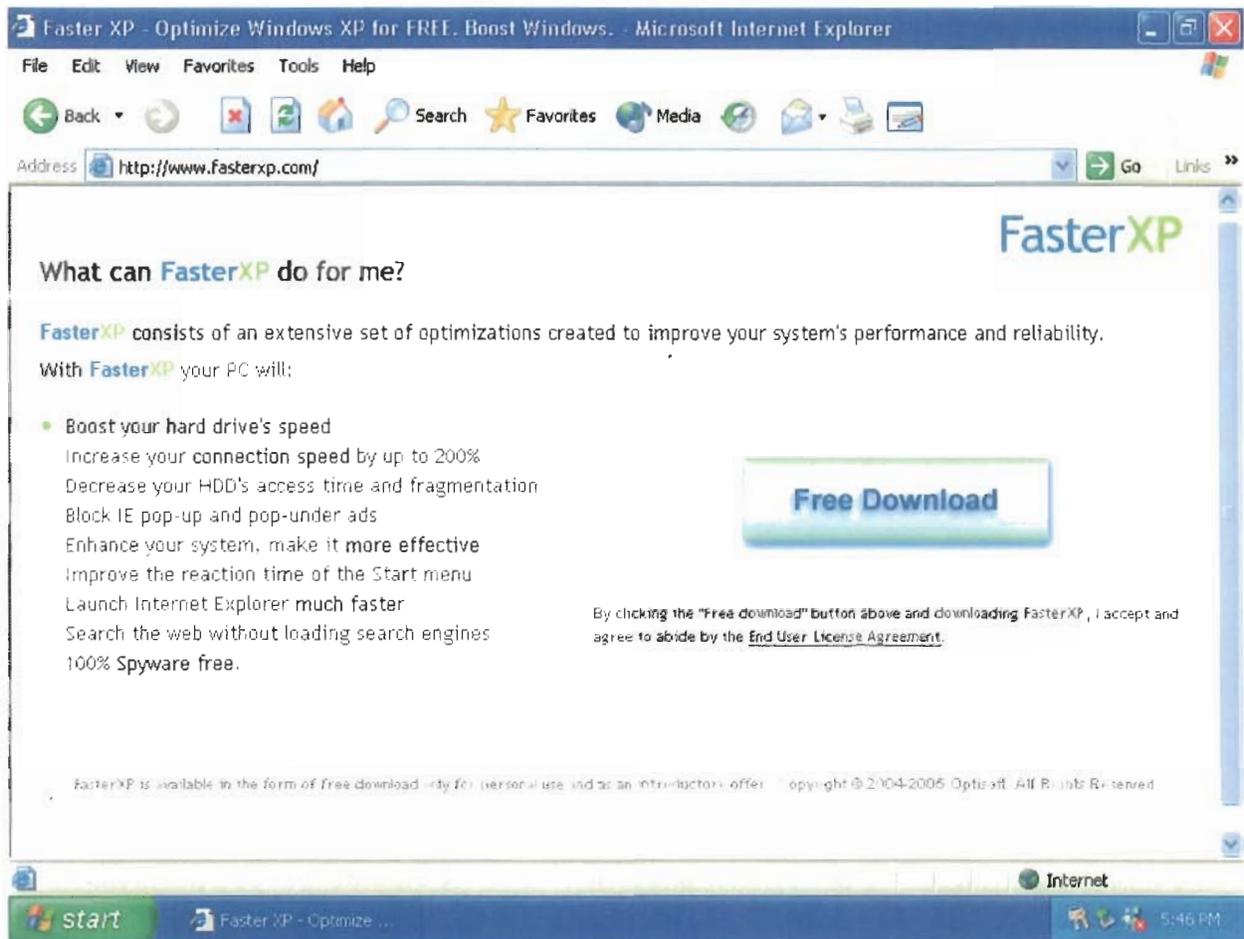
25. One third-party distributor that Direct Revenue has used to spread its spyware is Optisoft, Inc. This company runs the website <http://www.FasterXP.com> which offers free software purporting to increase hard drive and internet connection speeds by up to 200%. See Ip

---

<sup>1</sup> Since we contacted Direct Revenue about our investigation in May 2005, the company has shut down its internal ABetterInternet.com site for the distribution of its spyware (see infra ¶¶ 42-52), launched a new internal site for distributing its software named BestOffersNetwork.com and claims to have improved disclosure on third-party sites that distribute Direct Revenue's programs.

Aff. ¶ 7. As shown in Screen Shot No. 1 below, it also promises to “Block IE pop-up and pop-under ads,” and that it is “100% Spyware free.” See id.

**SCREEN SHOT NO. 1**



26. On May 11, 2005, an OAG investigator visited FasterXP.com to download this software program. After clicking on the “Free Download” icon shown in Screen Shot No. 1, the investigator arrived at a screen promising that the software was “100% Virus Free,” “100% Spyware Free” and “100% Trojans free.” See Ip Aff. ¶ 7. Next, a small dialog box popped up on the screen asking whether to Open, Save or Cancel the installation of the program. See id. ¶¶ 9-

11. Once this program was downloaded (by clicking “Open” or “Save”), the FasterXP software guided her through the installation of the software. This process consisted of several screens, each asking questions about connection to the internet and what sorts of settings the FasterXP program had authority to change on her computer. See id. ¶¶ 12-16.

27. None of the screens viewed by the investigator on the FasterXP site – nor any of the fifteen separate installation screens – made any mention of, or provided any hint regarding, Direct Revenue’s bundled spyware.

28. In order to maintain, however disingenuously, the charade of notice and consent, FasterXP’s License Agreement made vague reference to a company named “ABetterInternet.”<sup>2</sup> See Ip Aff. ¶ 8. This “License Agreement” was not, however, actually presented to the investigator. Rather, it was linked to the FasterXP.com home page, by a statement in small print reading: “By clicking the ‘Free Download’ button above and downloading FasterXP, I accept and agree to abide by the End User License Agreement.” See supra Screen Shot No. 1 (fine print across from the statement “100% Spyware free” (emphasis in original)); Ip Aff. ¶ 7.

29. No ordinary consumer downloading a free software program is likely to read such a license agreement – a document generally reserved for such dry legalities as copyright restrictions, limitations on liability, and choice of forum clauses. Certainly, no ordinary

---

<sup>2</sup> Although this fact is not disclosed to users who visit the FasterXP site, ABetterInternet is a subsidiary of Direct Revenue. See Exh. 7 (chart of Direct Revenue subsidiaries); Exh. 2 at 18-19. Emails among Direct Revenue executives indicate that they have set up numerous corporate entities in order to confuse angry customers about the origin of the company’s spyware and to diffuse responsibility. See Exh. 8 (email from D. Doman to J. Abram, A. Murray et al. dated August 26, 2004) (discussing setting up new company “that is not associated with Direct Revenue”); id. (“Josh [Abram] – I believe you are the master of this game.”); Exh. 9 (email from J. Abram to A. Murray dated February 13, 2004) (discussing setting up new companies and DBAs to disguise source of Direct Revenue distribution).

consumer would expect the only disclosure about bundled spyware to appear deep within such a document.

30. The FasterXP license agreement ran over 7000 words, spanning 12 separate screens. See Ip Aff. ¶ 8. The only hint of bundled software was a single statement on page four of the document reading: “Please read and understand the ABetterInternet End user license agreement before installing FasterXP, by clicking the following link <http://www.abetterinternet.com/policies.htm>.” See id. Only users who happened to scroll down to and open this hidden “link within a link” and then read the second agreement, might eventually learn that Direct Revenue spyware programs would be installed. See id.

31. Thus, no consumer would ever know he was downloading Direct Revenue’s spyware unless he first:

- Disregarded the initial, presumably complete, description of FasterXP’s software;
- Ignored the multiple promises that the FasterXP software was “100% Spyware Free,” “100% Virus Free” and “100% Trojans free”;
- Located the link for FasterXP’s “License Agreement”;
- Reviewed the “License Agreement” for FasterXP;
- Located the link to ABetterInternet.com within this License Agreement;
- Visited ABetterInternet.com’s web site;
- And then reviewed the second, nine-page license agreement posted on that site.

Clearly, no ordinary or reasonable consumer would think to undertake such an extraordinary investigation before downloading a free software program; indeed, most would not proceed beyond the first or second of the above steps.

32. Despite this utter lack of meaningful disclosure or consent, **Direct Revenue** installed its **Aurora** program on the test computer after the OAG investigator downloaded **FasterXP**. See **Ip Aff.** ¶¶ 17-21. Immediately, the investigator's test computer began receiving a litany of **pop-up ads** from **Direct Revenue** clients. See **id.** ¶¶ 19-20.

33. **Direct Revenue** was aware of the **deceptive lack of disclosure** provided on **FasterXP.com**. When a well-known **internet security expert** lambasted the company for this practice, **Direct Revenue** executives shrugged off the criticism with the **inexplicable** conclusion, "We are not **Spyware**." See **Exh. 10** (email from **D. Doman** to **J. Abram et al.** dated **May 21, 2005**). See also **Exh. 50** (email from **J. Cohen** to **D. Doman** dated **May 11, 2005**) (forwarding criticism of similar distribution practice where **Direct Revenue's spyware** was **disclosed** only through a link in another program's **EULA**).

34. Since **November 2003**, **Direct Revenue** installed over **400,000** of its **spyware** programs using this particular distributor. See **Exh. 2** at **Schedule 2**.<sup>3</sup>

Deceptive Installation from IEPrivacy.com

35. Another website **Direct Revenue** has used to secretly distribute its **spyware** programs is <http://www.IEPrivacy.com>. This website is operated by **Direct Revenue's** distributor **Skyhorn.com, Inc.** See **Exh. 11** (screen shot from **Skyhorn.com**). The site offers users a free privacy utility that, *inter alia*, deletes web browsing history and cookies from a computer's memory (presumably to prevent other users of the same computer from later discovering what

---

<sup>3</sup> **Optisoft, Inc.** also apparently **bundled** **Direct Revenue's spyware** programs with its **peer-to-peer, file-trading** software **Blubster**. In testing the disclosures made in downloading the **Blubster** software, an OAG investigator found reference to **ABetterInternet's** license hidden deep within **Blubster's** own license agreement, **without any other reference to** **Direct Revenue** or any **bundled spyware** programs. See **Thomas Aff.** ¶¶ 149-153.

sites the user had visited). See Thomas Aff. ¶ 126. On June 24, 2005, an OAG investigator downloaded and installed IEPrivacy.com's free privacy program, and confirmed that Direct Revenue had also silently installed its spyware, as described below.

36. As shown in Screen Shot No. 2 below, IEPrivacy's home page described in detail its privacy software, warning users that without it, others could easily learn what sites they had visited. See Thomas Aff. ¶ 126. The site also promised repeatedly that its software was "100% FREE." However, the page contained no mention whatsoever about any Direct Revenue spyware programs.

**SCREEN SHOT NO. 2**



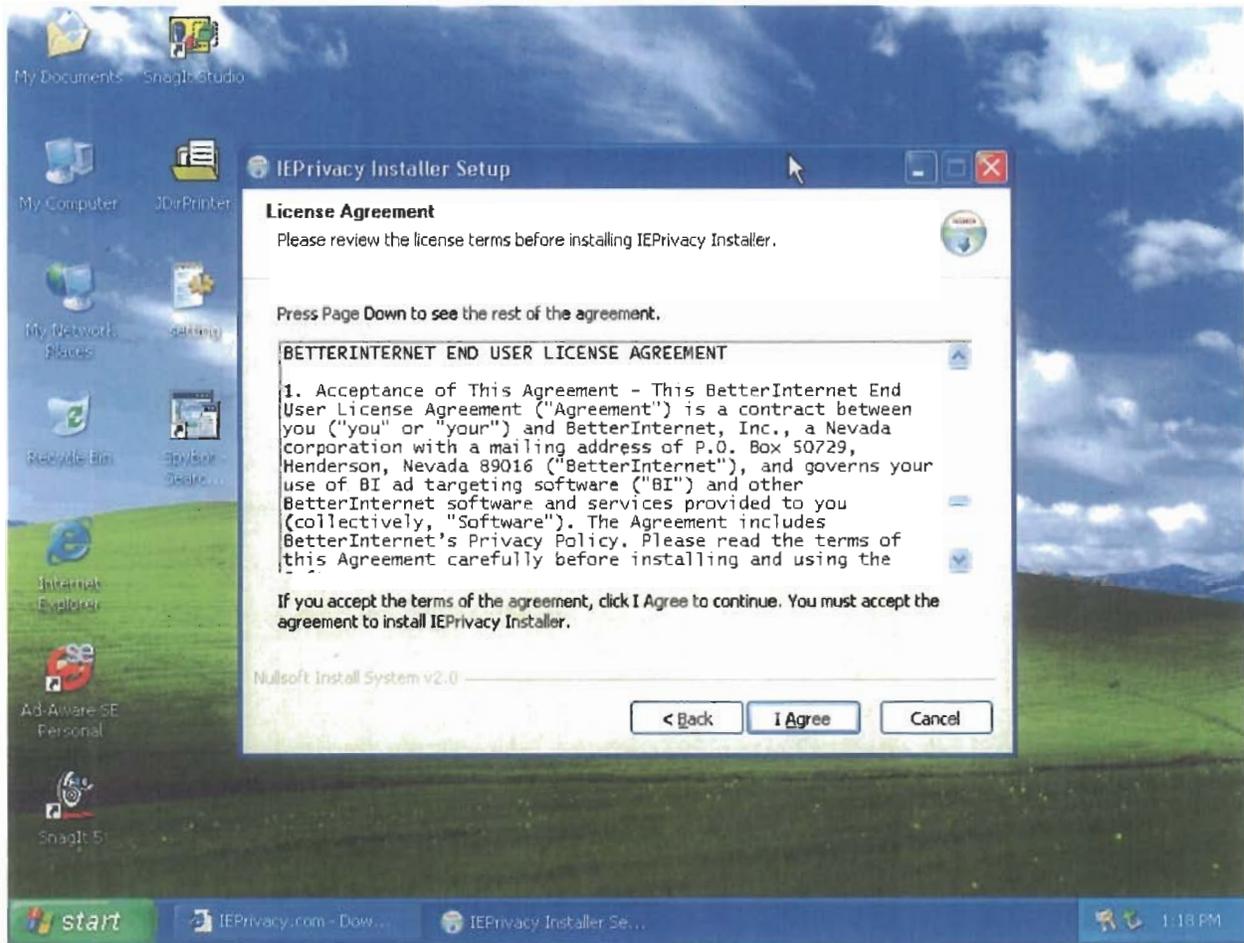
37. After clicking one of the many “Download” links on the above home page, the investigator arrived at a web page promising, “This is a FREE and safe download and is certified by Microsoft Authenticode,” and providing a pop-up box instructing the user to Open, Save or Cancel the installation of “IEPrivacy-install.exe.” See Thomas Aff. ¶¶ 127-28. Still, there was no notice or disclosure about any other bundled software programs.

38. After IEPrivacy’s “privacy” software was downloaded to the test computer, the

investigator clicked through several set-up screens to complete installation. See Thomas Aff. ¶¶ 129-31. Even these screens contained no meaningful notice of the bundled spyware. Rather, as with FasterXP.com, supra, notice about Direct Revenue's software was buried deep within a long, legalistic license agreement that any ordinary consumer would be unlikely to read in any detail.

39. Specifically, one of the several installation screens presented IEPrivacy's "End User License Agreement." See Thomas Aff. ¶ 130. This massive Agreement was contained within a small, difficult-to-read window that could not be expanded by the user. Most of its bulk was devoted to typical provisions such as limitations on liability, disclaimers of warranty and various license restrictions. See id. Finally, on the 131st of 188 screens, our investigator came to a section titled "BetterInternet License Agreement." See id.; Screen Shot No. 3, below. This section ran over 50 additional screens and did not even identify what software would be installed; it only stated that a company called "BetterInternet, Inc." had the right to install pop-up software and other undefined "Third Party Software." See id. As with FasterXP, supra, only a user who pored over the license agreement might learn that sophisticated spyware was about to load itself onto the user's computer. Obviously, no ordinary consumer would take such extraordinary investigative measures.

**SCREEN SHOT NO. 3**



40. After installation of the IEPrivacy program, tests confirmed that Direct Revenue’s Aurora pop-up program had been installed on the investigator’s test computer. See Thomas Aff. ¶¶ 137-39. The computer also began receiving a steady stream of pop-up advertisements for Direct Revenue’s clients’ products and services. See id. ¶¶ 133-35, 140.

41. Although the respondents suspected that Skyhorn used deceptive methods to install its spyware, Direct Revenue continued to use Skyhorn to as a distributor. See, e.g.,

Exh. 12 (email from M. Stanghed to J. Abram, A. Murray, D. Kaufman, R. Hook dated April 27, 2005) (joking that Skyhorn was installing Direct Revenue through “browser exploit [vulnerability] with 10 other people [i.e., other spyware companies] or the like”). Since February 2003, Direct Revenue has installed at least 370,000 of its spyware programs through Skyhorn, Inc. See Exh. 2 at Schedule 2.

#### Deceptive Installations from Sites Operated by Direct Revenue

42. Direct Revenue distributes much of its spyware using third parties such as Optisoft and Skyhorn, described supra. Direct Revenue also installs its spyware using its own proprietary web sites, such as ABetterInternet.com. Although Direct Revenue designed this site merely as a showpiece to demonstrate atypical “polite installs” to investors and other interested parties, see Exh. 13 (email from C. Dowhan to R. Khan dated July 14, 2004), the company eventually resorted to the same deceptive silent bundling tactics to trick consumers into installing its spyware.

43. ABetterInternet.com offered free programs for download, such as tools to eliminate spam or delete internet browsing history. See Exh. 14 (allwhois.com registration listing).<sup>4</sup> The website repeatedly emphasized that its programs were free, advertising, e.g., “THE BEST FREE DOWNLOADS ON THE WEB!” See Ip Aff. ¶ 39.

44. One program offered at ABetterInternet.com, called “Atomic Clock,” promised to correct the “internal clocks” of users’ computers by syncing them with the “US Government

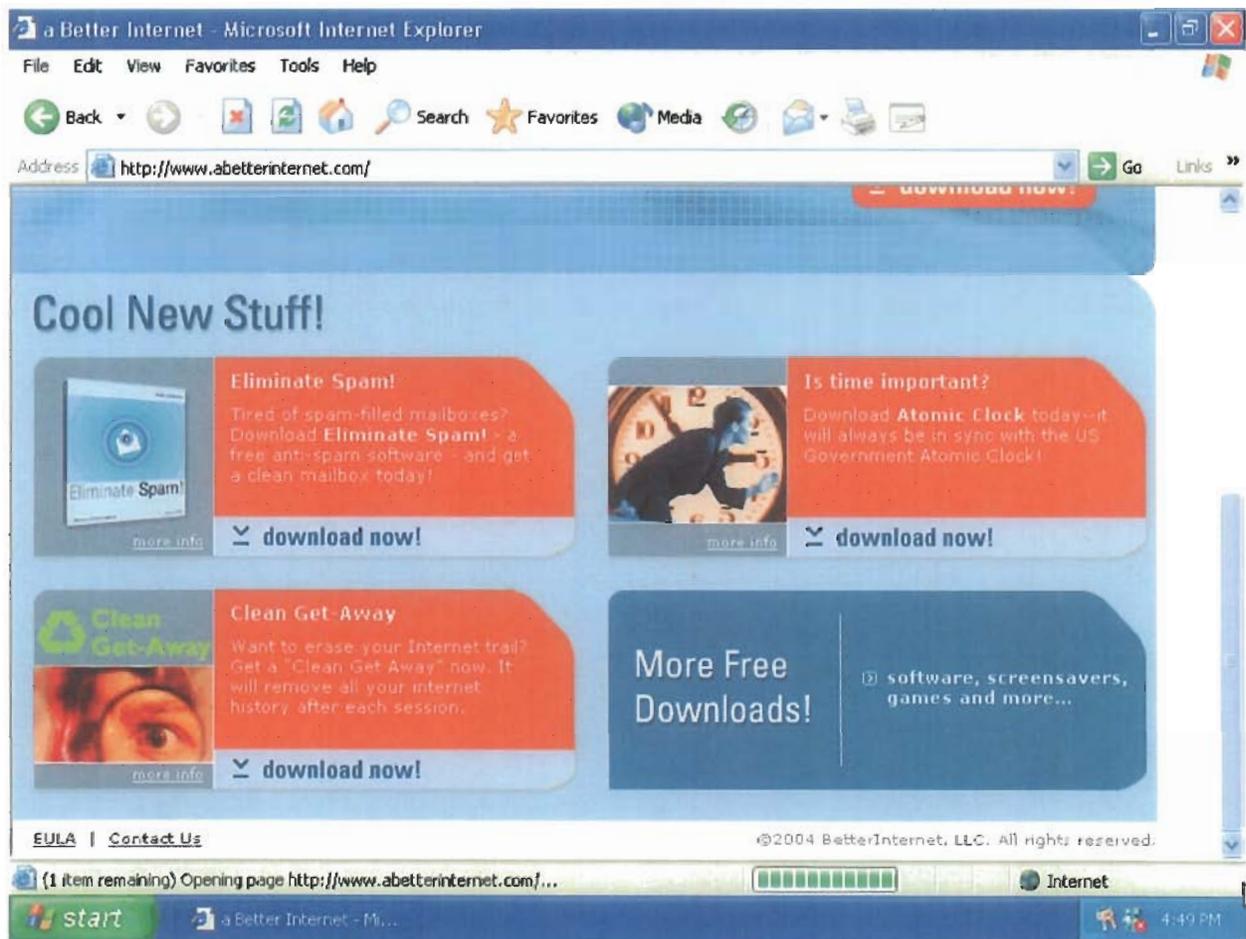
---

<sup>4</sup> Although the site is officially registered to “Thinking Media LP,” this entity is simply one of the many corporate names used by Direct Revenue to disguise its identity. See Exhs. 2 & 7; supra fn.2. See also Exh. 15 (email from D. Doman to A. Murray, R. Hook et al. dated August 30, 2004) (asking whether Thinking Media LP was “one of the fake companies that Josh [Abram] set up”).

Atomic Clock.” (The program is of dubious value, because nearly all operating systems automatically and regularly sync a user’s computer to a centralized clock on a regular basis.)

45. On January 13, 2005, an OAG investigator downloaded “Atomic Clock” from ABetterInternet.com. See Ip Aff. ¶¶ 37-54. As shown below in Screen Shot No. 4, the software was prominently featured on the ABetterInternet homepage. See id. ¶ 39. The page did not disclose, however, that it would come bundled with Direct Revenue’s spyware. See id.

**SCREEN SHOT NO. 4**



46. When the investigator clicked the “download now!” icon, a window popped up,

stating: “Install in progress . . .” See Ip Aff. ¶ 41. This page, too, omitted reference to bundled spyware. See id. The website then popped up a small dialog box encouraging the user to: “install and run the latest version of Atomic Clock . . . By clicking ‘Yes,’ you acknowledge that you have read and understand BetterInternet’s Consumer Policy Agreement and agree to be bound by its terms.”<sup>5</sup> See id. The box also stated, “BetterInternet asserts that this content is safe.” See id.

47. The dialog box, too, omitted any reference to bundled spyware programs, and the referenced “Consumer Policy Agreement” was not shown. In fact, it was wholly unavailable: when our investigator clicked on the hypertext link within the dialog box, the computer reported that the requested page could not be found. See Ip Aff. ¶ 42. But even if the “Consumer Policy Agreement” had been available, no ordinary consumer would expect the sole notice of a bundled spyware program to be within such a document.

48. After the investigator clicked “Yes” on the consent box, several more installation screens appeared to complete the installation of the Atomic Clock software. None of these screens contained any mention of bundled spyware programs. See Ip Aff. ¶ 44.

49. Despite the absence of notice or consent, tests immediately following this installation of Atomic Clock showed that Direct Revenue’s Ceres pop-up program had been silently installed on our test computer. See Ip Aff. ¶ 47-50.

50. According to records from Archive.org (a website that records for posterity

---

<sup>5</sup> However, if a user’s Internet Explorer security settings were set to “low,” the user would not even see this dialog box, and the programs (including the bundled spyware) would install automatically and without notice. See Exh. 20 (Transcript of the § 63(12) Hearing of Christopher Dowhan (“Dowhan Tr.”)) at 24-26; infra ¶¶ 60-62 (discussion of ActiveX technology).

snapshots of well-trafficked websites), ABetterInternet.com has remained substantively as described above since at least June 2004. See Thomas Aff. ¶¶ 142-148 (describing archived images of the ABetterInternet home page).<sup>6</sup> Although Archive.org's records do not reveal whether or at what dates the linked "Consumer Policy Agreement" may have been available for review, it is unreasonable in any event to expect that any ordinary consumer would review such a document for notice of hidden, bundled spyware programs.

51. Direct Revenue estimates that it has distributed several thousand spyware programs from its ABetterInternet.com website. See Exh. 6 (letter from N. Klausner to K. Dreifach et al. dated January 17, 2005) at 9-10.

52. OAG investigators documented similar deceptive methods of distribution at the Direct Revenue website MyPanicButton.com (offering a program that disguises personal use of the computer in a work environment). See 1p Aff. ¶¶ 55-72; Exh. 17 (whois registration listing). To date, Direct Revenue has not disclosed how many programs it has distributed through this site.

Deceptive Installation from MyTracksEraser.com

53. Direct Revenue has used similar tactics to silently distribute its spyware to

---

<sup>6</sup> The example provided in the Declaration of Christopher Dowhan, Direct Revenue's Vice-President for Distribution, in another legal proceeding documents the same absence of disclosure on the ABetterInternet.com website. The link to the "Consumer Policy Agreement" was described as operational in that instance. See Exh. 16 at 3-4 & Exhibit C. The Declaration does point out, however, that for users with Microsoft Windows's "Service Pack 2" security upgrade installed, users were not even shown the language that they were implicitly agreeing to Direct Revenue's "Consumer Policy Agreement." Instead, those users only saw a confusing dialog box reading, "The site might require the following ActiveX control: 'the latest version of Flashtalk? By clicking . . . from BetterInternet?' Click here to install." See id. at 4-7 & Exhibit D (ellipsis in original).

unsuspecting consumers through the site MyTracksEraser.com. This site, operated by Direct Revenue distributor Holystic, Ltd., offers “free” software promising features similar to the FasterXP and IEPrivacy programs described previously: e.g., “stop people finding out where you have been,” “speed up your internet surfing and protect your privacy” and “clean your PC and make it work faster.” See Ip Aff. ¶ 101. The MyTracksEraser.com home page also promises repeatedly that the software is “100% Free.” See id.

54. On July 6, 2005, an OAG investigator visited this website and downloaded the “free” privacy software by clicking a link reading “DOWNLOAD NOW 100% FREE.” See Ip Aff. ¶ 104. Neither the MyTracksEraser home page, nor any screen shown during the installation process, made any mention whatsoever of any bundled spyware programs. Nevertheless, after installing the MyTracksEraser software, our investigator confirmed that Direct Revenue’s Aurora spyware program had been installed on her computer. See id. ¶¶ 108-111.

55. In addition to its MyTracksEraser site, Holystic sometimes installed Direct Revenue’s spyware bundled with adult “dialer” programs. See Exh. 18 (email from S. Morris to J. Abram, A. Murray et al. dated December 21, 2004). Dialer programs disconnect users who connect to the internet with a dial-up modem, and reconnect them to a different phone number, usually at a significantly higher cost. They are predominantly associated with adult, pornographic websites. Tests conducted by an OAG investigator confirm that Direct Revenue was bundled with Holystic’s adult dialer programs – without notice to users. See Ip Aff. ¶¶ 128-147. In fact, even after the investigator cancelled the installation of the dialer program, Direct Revenue’s spyware was silently installed on the test computer. See id. ¶¶ 139-141.

56. Direct Revenue has installed more than 245,000 of its spyware programs through

Holystic. See Exh. 2 at Schedule 2.

#### Deceptive Installations from Net Think Media Websites

57. Direct Revenue also has distributed its spyware programs through websites operated by Net Think Media (d/b/a Fabian Buys). OAG investigators captured installations of Direct Revenue's spyware programs on two such websites, PCWeatherAlert.com (offering a free program to deliver weather alerts to a user's desktop) and TaskBuddy.com (offering free organizational software to help coordinate tasks and to-do lists).

58. As in the prior examples, when the investigator downloaded the promised software, it came bundled with Direct Revenue's spyware. This occurred without any notice to the user, either on the initial web pages, during download and installation, or even through a linked EULA or "terms of service." See Ip Aff. ¶¶ 203-247.

59. Direct Revenue installed its spyware through sites owned by Net Think Media over 190,000 times since February 2003. See Exh. 2 at Schedule 2.

#### Deceptive Downloads Through Mindset Interactive

60. In the above examples, Direct Revenue's spyware came bundled with other, purportedly "free" software, after users had visited certain websites to download the "free" software. In a variation on this theme, Direct Revenue sometimes distributes its programs through "ActiveX" advertisements, which are hosted on web sites with content wholly unrelated to software downloads. See infra Screen Shot No. 5 (example of an "ActiveX" advertisement).

61. Specifically, Direct Revenue (or its distribution partners) hire ad networks to place these "ActiveX" advertisements on host websites. These ActiveX ads and installations are even more aggressive than the bundle downloads described above, because they are not user-

initiated. Rather, ActiveX dialog boxes, labeled as “security warnings,” pop up on unrelated web sites, offering users such programs as games, internet phone services, or undefined “browser enhancements.” The advertisements fail to mention that the consumer will also receive one or more bundled spyware programs.<sup>7</sup>

62. If a user’s Internet Explorer security settings are set to “low,” the user will not even see the pop-up consent box when an ActiveX advertisement runs. Instead the “advertised” program will download and install automatically, along with any bundled spyware. See Exh. 20 (Transcript of the § 63(12) Hearing of Christopher Dowhan (“Dowhan Tr.”)) at 61-62; Exh. 21 (excerpt from *Malware: Fighting Malicious Code* by Ed Skoudis). For older versions of Microsoft’s Internet Explorer program, the default security setting automatically runs and installs ActiveX programs without any interaction with the user. See id. Thus, by merely visiting a website hosting an ActiveX “advertisement,” users can become infected with Direct Revenue’s spyware programs. See infra ¶ 77.

63. Several examples of “ActiveX” downloads are described below. These examples

---

<sup>7</sup> Microsoft originally designed and introduced “ActiveX” technology to allow web designers to integrate small programs into their web pages to make web pages dynamic and interactive. Macromedia’s “Flash” and “Shockwave” programs are typical ActiveX programs which allow web designers to display animated content to visitors to their site. Distributing ActiveX programs for unrelated software programs – let alone spyware programs – across advertising networks is thus a very controversial practice, as it perverts Microsoft’s benign intent in incorporating the technology into their Internet Explorer web browser.

Direct Revenue executives have recognized that this method of distributing its spyware programs abuses Microsoft’s ActiveX technology. Upon hearing a suggestion that Direct Revenue partner with Microsoft, Direct Revenue’s Chief Technology Officer commented: “I doubt that they want to partner with someone who actually takes advantage of their vulnerability and poor design.” See Exh. 19 (email from D. Doman to T. Phillips dated September 17, 2004).

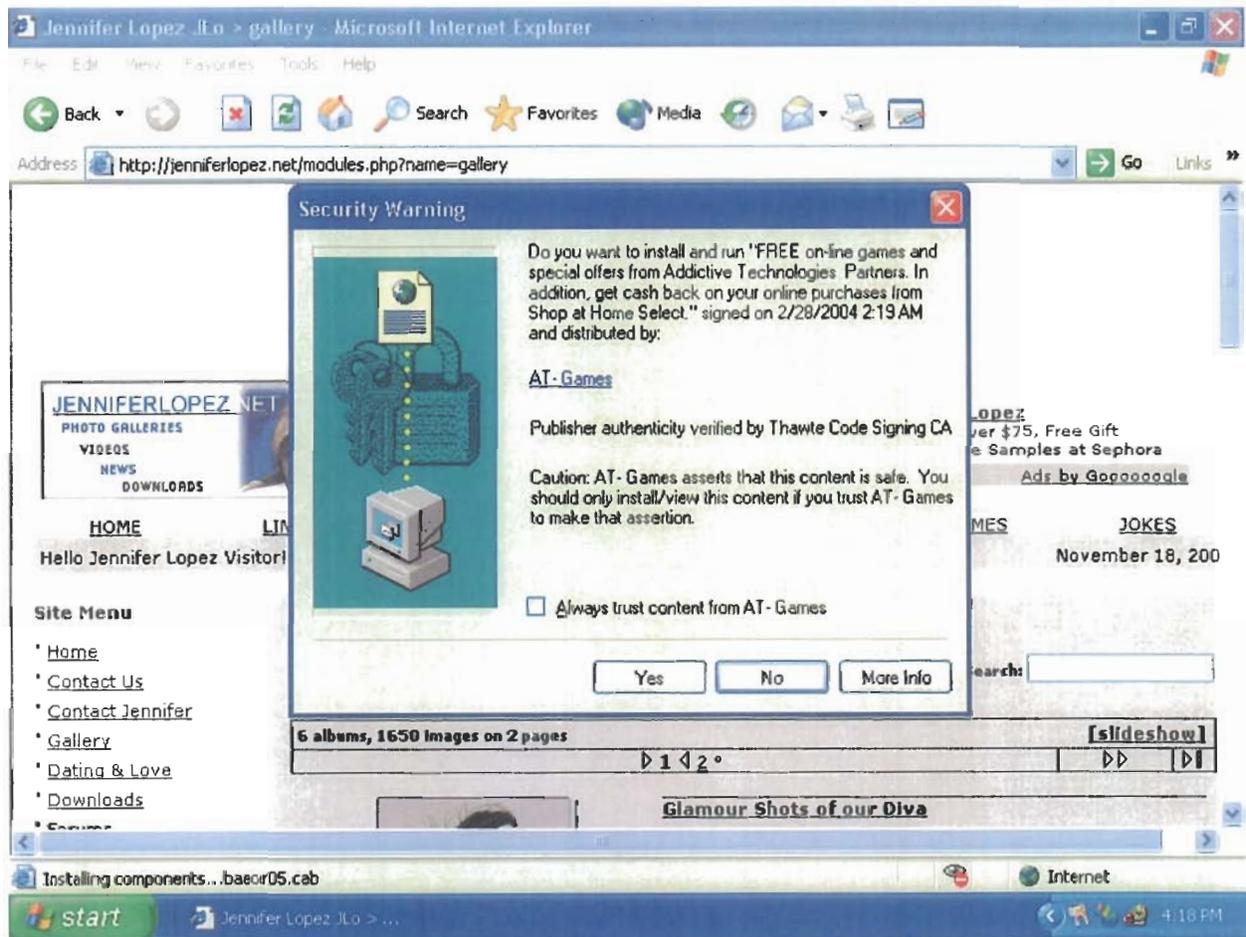
reflect the disclosures shown when a user's security settings are sufficiently high to trigger the ActiveX "Security Warning."

64. For instance, when an OAG investigator visited the fan site <http://www.JenniferLopez.net> on November 18, 2004, an ActiveX advertisement authored by Mindset Interactive ("Mindset")<sup>8</sup> triggered a "Security Warning" ActiveX box on her test computer. This ActiveX box offered: "FREE on-line games and special offers from Addictive Technologies Partners. In addition, get cash back on your online purchases from Shop at Home Select." See Ip. Aff. ¶ 191. This "Security Warning," shown below as Screen Shot No. 5, made no mention Direct Revenue's spyware. See *id.*

---

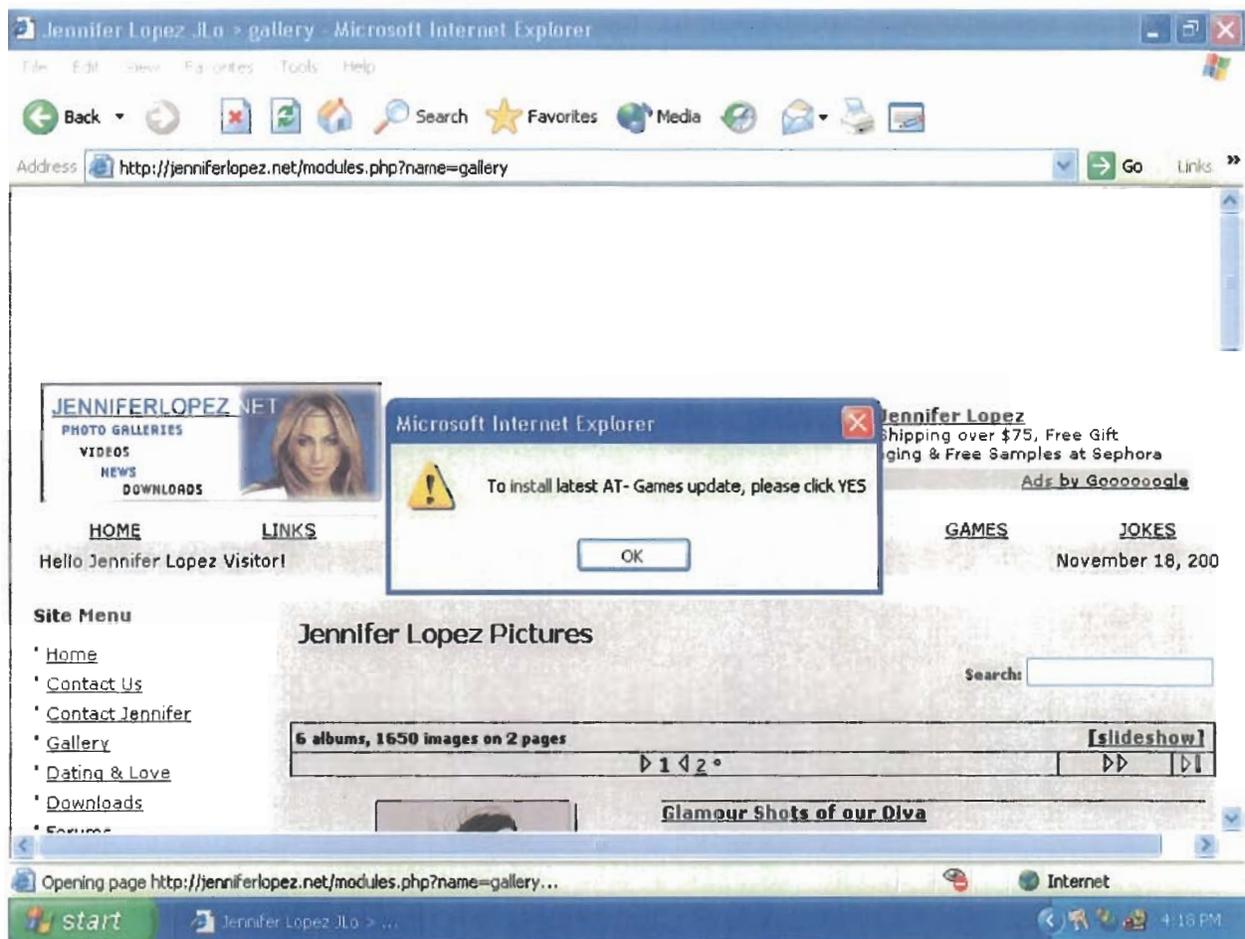
<sup>8</sup> Mindset owns and operates Addictive Technologies, the identified author of this particular ActiveX program. See Exh. 22 (archive.org screen shot of <http://www.addictivetechologies.com>). (The precise relationship between Mindset and the proprietors of the JenniferLopez.net website is not known at this time, but presumably Mindset paid the proprietor of the site to host the ActiveX "advertisement," either directly through an affiliate program or through a third-party ad network.) Direct Revenue paid Mindset directly to distribute its spyware programs in this manner. See Exh. 23 (identifying payments of over \$1,000,000 made by Direct Revenue to Mindset Interactive between May 2004 and April 2005).

**SCREEN SHOT NO. 5**



65. When the investigator clicked “No” (i.e., do not install) to this download prompt, a second dialog box popped up, stating: “To install latest AT-Games update, please click YES.” See Ip. Aff ¶ 195. Again, as shown below in Screen Shot No. 6, there was no mention of any Direct Revenue software. See id.

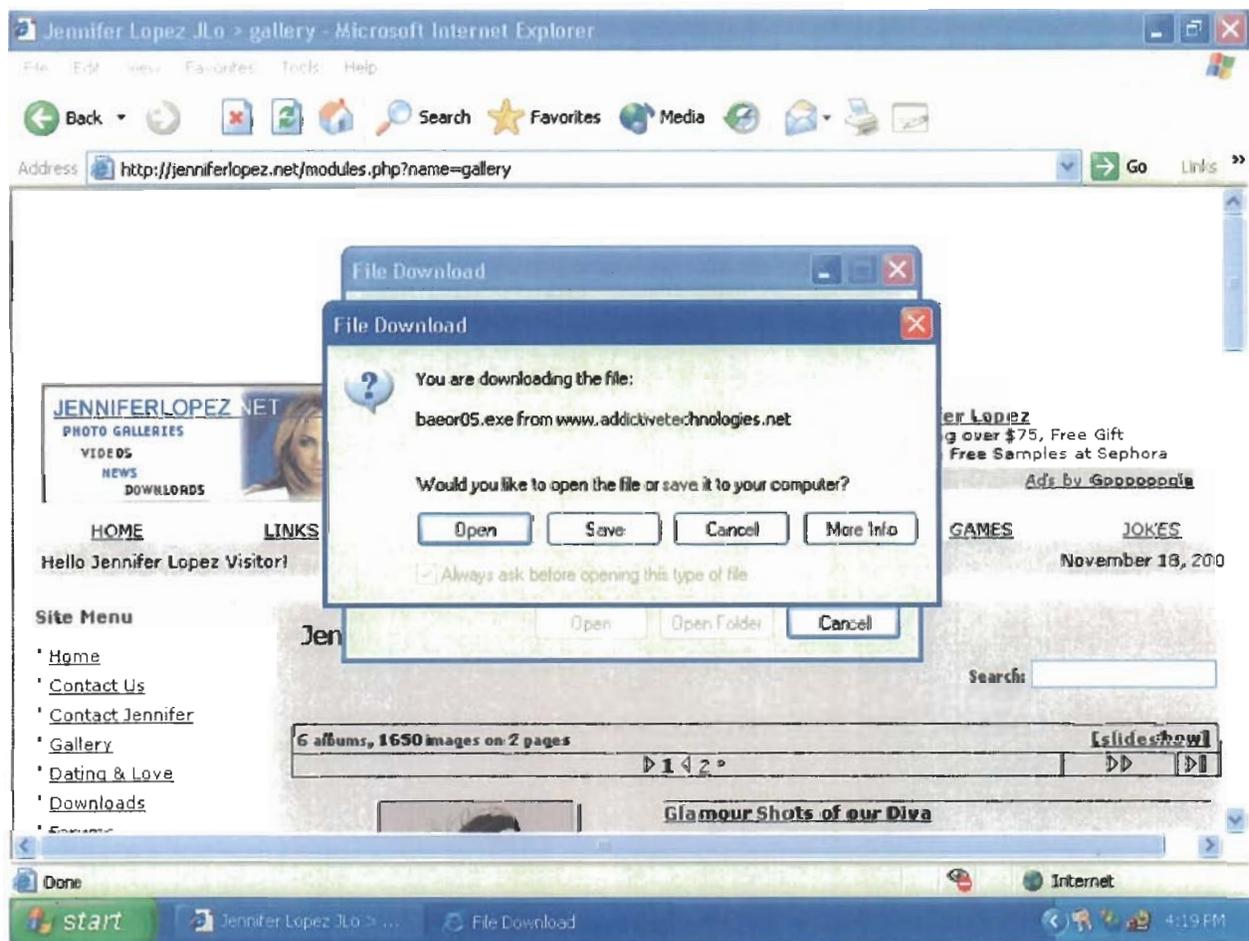
## SCREEN SHOT NO. 6



66. When the investigator tried to close that pop-up box (offering installation of “AT-Games update”), the first ActiveX security box popped up once more, again offering “FREE on-line games and special offers from Addictive Technologies Partners.” See *Ip. Aff.* ¶ 196. Again, the investigator clicked “No.” In response to this second rejection, yet another pop-up box appeared, offering: “This is a 1 time install, once you click Open it will never pop up this message again.” See *id.* ¶ 197. Our investigator again closed the Javascript prompt.

67. Despite these repeated rejections, the malicious program continued to attempt to install itself. Next, a pop-up box, shown below as Screen Shot No. 7, informed our investigator that a file identified as “baeor05.exe from addictivetechologies.net,” was being loaded onto the computer, and asked “Would you like to open the file or save it to your computer.” See Ip Aff. ¶ 198. Even then, no description of Direct Revenue spyware, or any other software, was provided. See id.

### SCREEN SHOT NO. 7



68. Even though the OAG investigator clicked “Cancel” to reject this installation,

several programs began to download and install on her test computer. See Ip Aff. ¶¶ 199-201. In tests performed immediately thereafter, our investigator determined that instead of the “free games” promised by the ActiveX security box (which she had never consented to install anyway), Mindset’s “FavoriteMan” spyware program had been installed.<sup>9</sup> FavoriteMan, in turn, had installed Direct Revenue’s spyware (among other programs). See id. ¶¶ 200-201.

69. At no point before, during or after the installation process was Direct Revenue’s spyware program identified or described. Indeed, in the investigator’s tests, she had not consented to install any software on her computer.

70. In three other tests of JenniferLopez.net, our investigator encountered the same dialog prompts described above. See Ip Aff. ¶¶ 202. (In the later tests, the investigator eventually consented to the installation of the “baeor05.exe” file seen in Screen Shot No. 7.) Despite the fact that Direct Revenue and its spyware programs were never mentioned or described, after each test, the investigator confirmed that Direct Revenue’s pop-up software had been installed on the test computer. See id.

71. Between August 2003 and May 2005, Direct Revenue installed over 16,000,000 programs through Mindset Interactive.

#### Deceptive Installation Through NicTech Networks

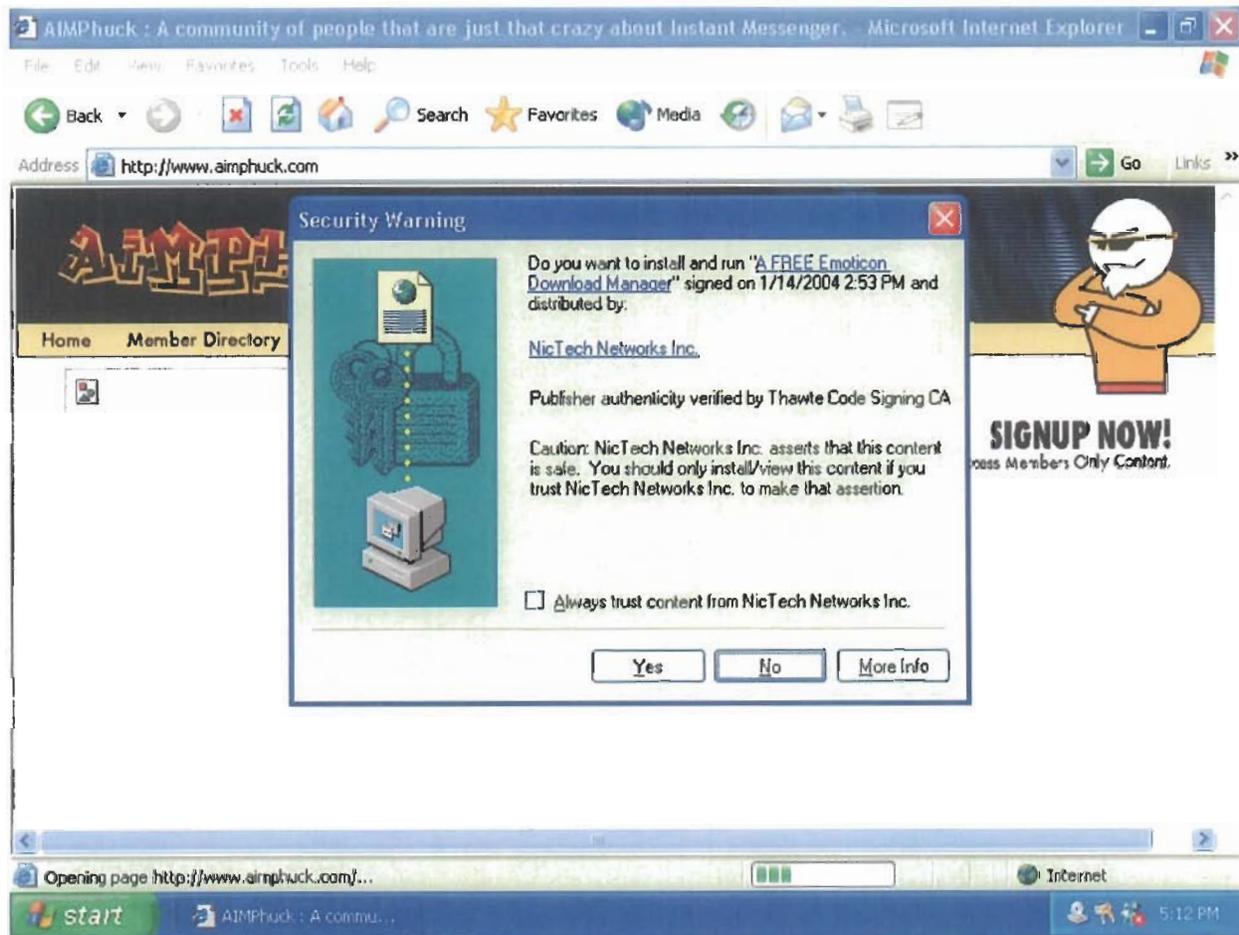
72. An OAG investigator recorded Direct Revenue installing its spyware through similar ActiveX advertisements from the company NicTech Networks. On January 27, 2005, the investigator visited AIMPhuck.com – a website offering icons and avatars targeted at teenagers

---

<sup>9</sup> “FavoriteMan” installs new icons on a user’s desktop and adds various links to the “Favorites” list in Internet Explorer; it also uploads and installs other spyware programs onto the computer’s hard drive.

who use instant messaging programs. See Ip Aff. ¶ 150. Immediately, an ActiveX “security warning” popped up asking “Do you want to install and run ‘a FREE Emoticon Download Manager?’” See *id.*; Screen Shot No. 8 below.<sup>10</sup>

### SCREEN SHOT NO. 8



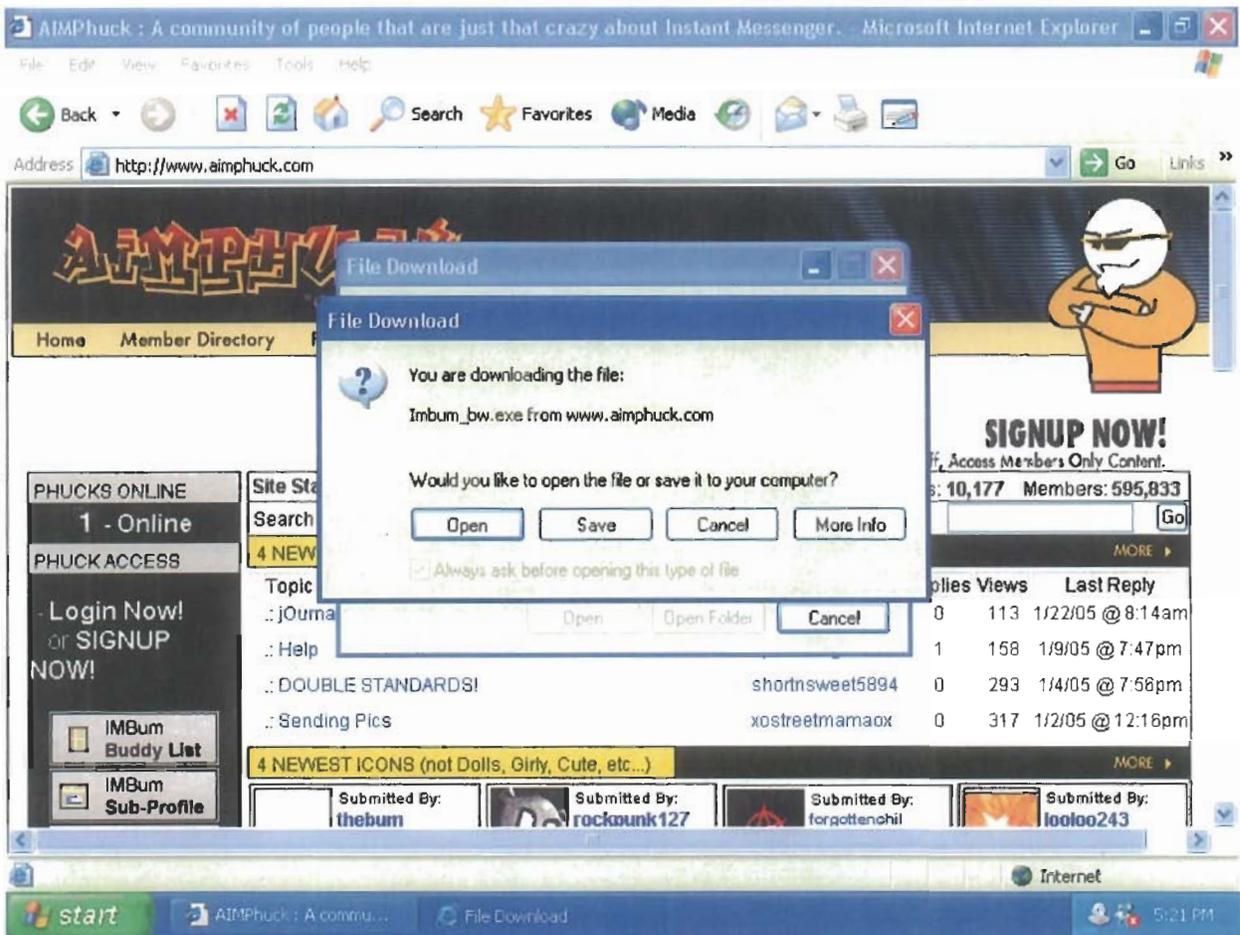
73. Plainly, there was no mention of bundled spyware contained in the advertisement. Although the investigator clicked “No” to reject installation, she was bombarded with non-stop

---

<sup>10</sup> “Emoticons” are small animations, such as a smiley face, that instant messaging users often include in their online conversations.

follow-up prompts, similar to those described above from Mindset Interactive. See Ip Aff. ¶¶ 150-156; supra ¶¶ 64-68. Finally, the investigator consented to download an undescribed file named “Imbum\_bw.exe from www.aimphuck.com.” See Ip Aff. ¶ 156; Screen Shot No. 9 below.

**SCREEN SHOT NO. 9**



74. When the investigator finally clicked “Open” to the above prompt, a number of programs were immediately installed on her test computer, including a pop-ad program from Direct Revenue. See Ip Aff. ¶¶ 161-165. No notice had been given about Direct Revenue’s bundled programs either before or after installation.

Deceptive Installations from Pacerd's "Free Browser Enhancements"

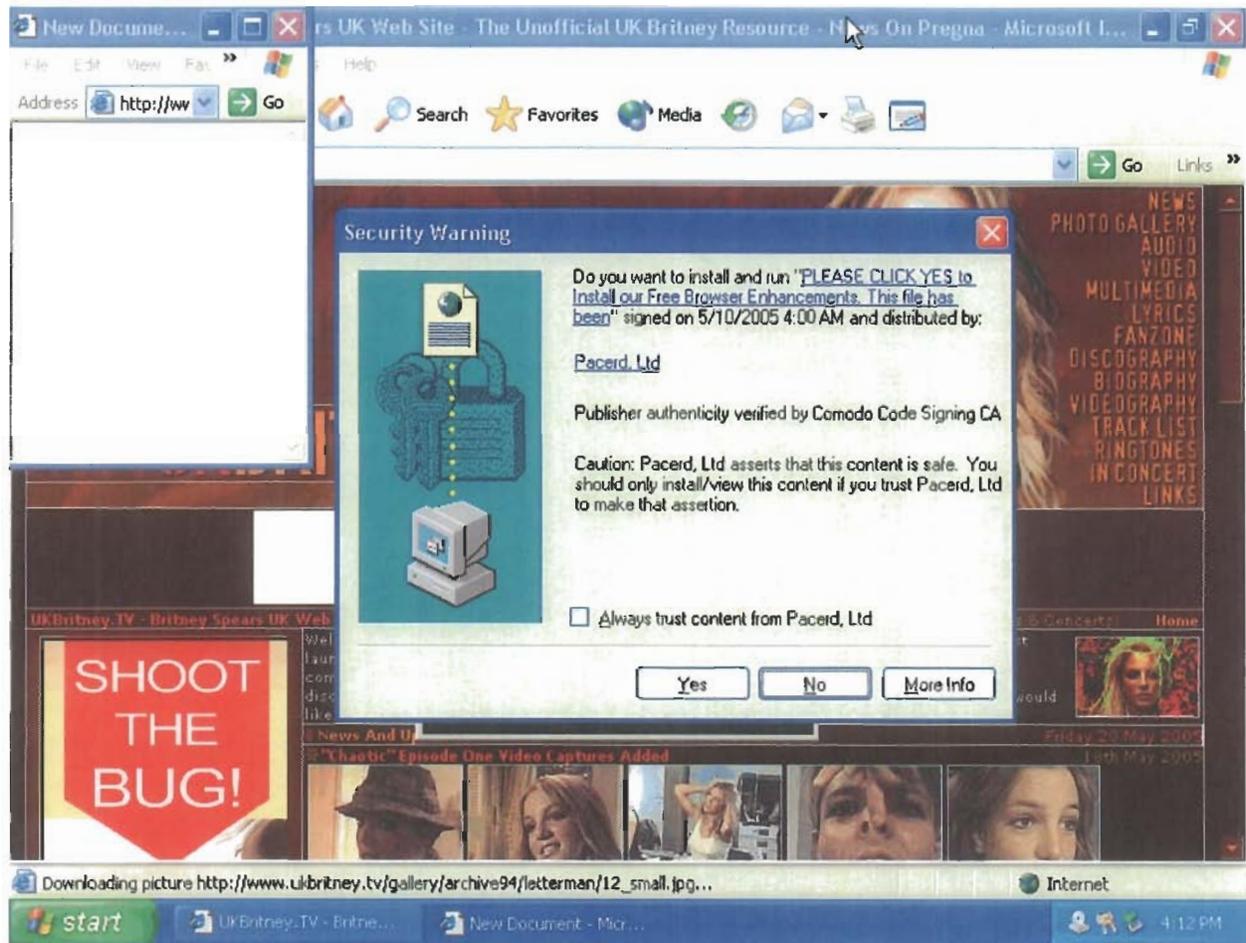
75. OAG investigators recorded Direct Revenue installing spyware through similarly deceptive "ActiveX" advertisements authored by the company Pacerd.<sup>11</sup> For instance, on May 23, 2005, an OAG investigator visited a Britney Spears fan site, <http://www.ukbritney.tv>. As shown in Screen Shot No. 10 below, an ActiveX "security warning" immediately popped up asking whether to install "Free Browser Enhancements." (These "enhancements" were not further described.) The "warning" also represented that the "Publisher authenticity [was] verified by Comodo Code Signing CA" and that "Pacerd, Ltd asserts that this content is safe."<sup>12</sup> The security warning contained no notice or description of any Direct Revenue spyware program. See Thomas Aff. ¶ 64.

---

<sup>11</sup> It is not known whether Pacerd or NicTech Networks have direct relationships or subdistributor relationships with Direct Revenue. It is conceivable that one of Direct Revenue's contracted distributors proceeded to subcontract the distribution of Direct Revenue's spyware to those companies. See *infra* ¶¶ 99-100 (discussing distributor subcontracting to subdistributors). Alternatively, it is possible that one of the other spyware programs installed by Pacerd or NicTech Networks may have silently bundled Direct Revenue's spyware.

<sup>12</sup> When our investigator clicked on the underlined text within the ActiveX "Security Warning," he was directed to a webpage that displayed a "Pacerd End User License Agreement." See Thomas Aff. ¶ 65. This document contained no reference whatsoever to Direct Revenue or its spyware programs. See *id.*

**SCREEN SHOT NO. 10**



76. When the investigator clicked “Yes” on the Security Warning, numerous spyware applications silently installed onto his test computer, including Direct Revenue’s Aurora pop-up ad program. See Thomas Aff. ¶¶ 66-72. No notice was provided at any point about bundled Direct Revenue spyware programs.

77. In another test of this same website, an OAG investigator visited this website with his Internet Security settings set to “Low.” See id. ¶¶ 77-78. In that test, the investigator was not shown any prompt regarding Pacerd’s “Browser Enhancements.” Instead, multiple spyware

programs, including Direct Revenue's Aurora, were installed on the test computer with no notice or opportunity for consent whatsoever. See id. ¶¶ 73-86.

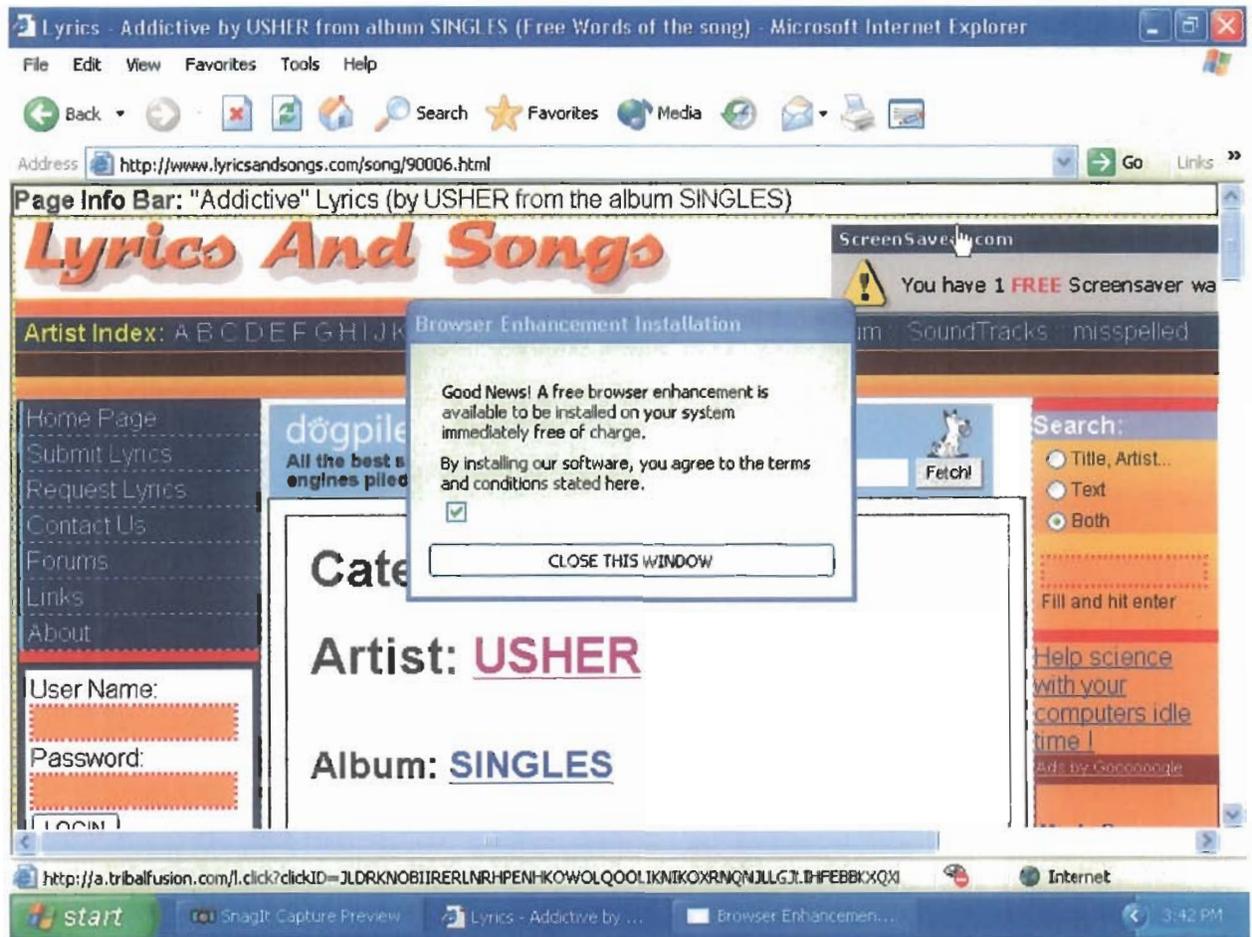
78. In visiting other web sites, OAG investigators encountered similar "ActiveX" boxes, promising this same "Browser Enhancement Software" in the guise of a Microsoft Security Warning. Upon accepting the Pacerd "Browser Enhancement" software (through pop-up ActiveX installation screens), the investigators recorded similar silent installations of Direct Revenue's spyware programs. See Ip Aff. ¶¶ 166-177; Rivela Aff. ¶¶ 44-55.

79. Other Pacerd "advertisements" that Direct Revenue has used to disseminate its spyware were even more egregious. Often, the dialog box presented did not even give consumers the option to reject the installation of the "Browser Enhancement" programs.

80. For instance, on August 3, 2005, an OAG investigator found a particularly deceptive Pacerd "advertisement" on <http://www.lyricsandsongs.com>, a site that provides lyrics to thousands of popular songs. See Rivela Aff. ¶¶ 22-33.

81. As soon as our investigator arrived at LyricsAndSongs.com, a small window, titled "Browser Enhancement Installation," popped up on his screen. See Rivela Aff. ¶ 27; Screen Shot No. 11, below. The window promised a "free browser enhancement" and noted that "[b]y installing our software, you agree to the terms and conditions stated here." However, there were no terms and conditions listed, nor was there even a link to another page containing any terms and conditions. The window did not even offer users a chance to click "Yes" or "No" to the installation; instead, there was only a large button reading: "CLOSE THIS WINDOW." See id.

SCREEN SHOT NO. 11



82. Because there was no obvious way to reject the installation of these “browser enhancements,” the OAG investigator **tried to abort the installation by pressing Ctrl, Alt and Delete simultaneously.** See Rivela Aff. ¶ 28. (This is a standard way to close unwanted programs, through Windows’ “Task Manager.”). See Rivela Aff. ¶ 29. Despite using Windows’s Task Manager to close the Pacerd “advertisement,” **Aurora and several other spyware programs were silently installed onto the test computer.** At no point **prior to or during**

installation was there any mention or disclosure of Direct Revenue spyware programs. See id. ¶¶ 27-33.

83. An OAG investigator encountered the very same “Browser Enhancement Installation” pop-up box on another site, <http://www.wallpapers4u.com>, which provides photographs and images that users can download as their computer’s “wallpaper,” or background. See Rivela Aff. ¶¶ 3-12. This time, the investigator simply clicked the “CLOSE THIS WINDOW” button. Again, Direct Revenue’s Aurora spyware program (along with other spyware) installed itself silently and without consent. See id. ¶¶ 7-12.

84. As described infra at ¶¶ 146-147, Direct Revenue’s officers knew that Pacerd was initiating Direct Revenue’s spyware downloads through these deceptive methods. Nevertheless, when OAG investigators tested Pacerd’s advertisements months after Direct Revenue’s officers discussed Pacerd’s practices, Direct Revenue’s spyware was still being distributed in precisely the same manner. See Rivela Aff. ¶¶ 3-12, 22-33, 44-54; Ip Aff. ¶¶ 166-177.

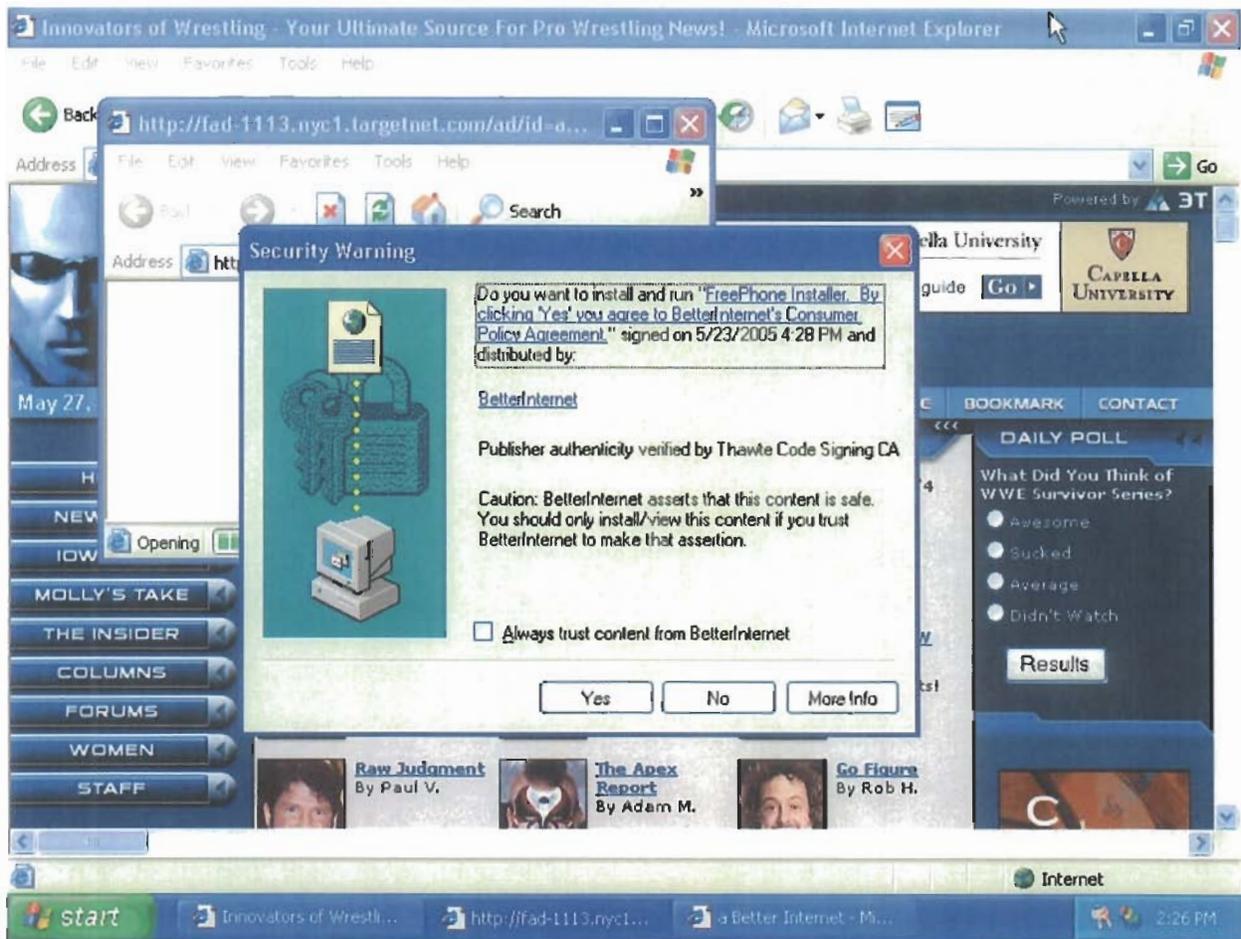
#### Deceptive Downloads Through Direct Revenue’s Own ActiveX Advertisements

85. In addition to bundling its spyware with third-party programs distributed through misleading ActiveX advertisements, Direct Revenue itself has used deceptive ActiveX advertisements to distribute its proprietary programs such as Atomic Clock (discussed supra at ¶¶ 42-49), screensavers and “FreePhone” (a program offering voice-over-internet phone service). See Exh. 24 (affidavit of Alan Murray). After disclosing only the advertised program to the user, Direct Revenue would silently install its bundled spyware programs as well.

86. For example, on May 27, 2005, an OAG investigator visited <http://www.IOWrestling.com>, a professional wrestling fansite. After entering the address for the

IOWrestling.com’s home page, an ActiveX “Security Warning,” shown at Screen Shot No. 12 below, popped up reading: “Do you want to install and run ‘FreePhone Installer. By clicking ‘Yes’ you agree to BetterInternet’s Consumer Policy Agreement.” See Thomas Aff. ¶ 92.

**SCREEN SHOT NO. 12**



87. When the investigator clicked “Yes” to the “Free Phone” installation box, Direct Revenue’s “FreePhone” downloaded and installed onto the test computer. See Thomas Aff. ¶ 94. The investigator was then guided through a laborious installation process to set up the

“FreePhone” program, which ostensibly would allow him to make phone calls over the internet. See id. ¶¶ 94-96. Nowhere during this installation process (nor prior to download) was it disclosed that bundled spyware programs also were being downloaded and installed. See id. Disclosure about the bundled spyware program was only provided if a user clicked on the link containing the BetterInternet “Consumer Policy Agreement.” See id. ¶¶ 92-93. Nevertheless, despite this lack of disclosure, the investigator confirmed that Direct Revenue’s “Aurora” spyware program had also been installed on his computer. See id. ¶¶ 97-105.

88. On other occasions, OAG investigators encountered similar ActiveX advertisements for Direct Revenue programs. In each instance, when a “Security Warning” was triggered and shown to the viewer, it mentioned only the advertised program (such as “FreePhone”) – omitting any reference to any bundled spyware programs. See Ip Aff. ¶¶ 178-187; Thomas Aff. ¶¶ 3-47. In each instance, undisclosed Direct Revenue spyware programs also were silently installed on the investigator’s test computer.

89. Through such deceptive ActiveX bundles, Direct Revenue has distributed its spyware nearly 10,000,000 times. See Exh. 6 (letter from N. Klausner to K. Dreifach et al. dated January 17, 2006) at 8-9.

#### Deceptive “Drive-by” Downloads

90. Worst of all, our investigation revealed instances in which Direct Revenue’s spyware was installed through security vulnerabilities in Microsoft’s web browser and operating system. This practice is known as a “drive-by download,” because software is maliciously installed without warning simply upon visiting a website – regardless of the user’s security settings.

91. On May 13, 2005, an OAG investigator visited <http://www.700xxx.com>. See Thomas Aff. ¶ 52. This website contained dozens of pornographic images, including graphic images of underage girls engaged in sexual activity. See *id.* When the investigator clicked any one of these pictures, the website immediately began to install (without any further prompting or interaction) several spyware programs onto the test computer, including Direct Revenue’s Aurora program. See *id.* ¶¶ 53-59. The investigator was never notified that spyware programs would be installed on the computer, nor was his consent ever requested. Investigators found similar “vulnerability installations” of Direct Revenue spyware on the pornographic website <http://www.ebs.fuck-access.com> as well as the site <http://www.crackz.ws>, which teaches how to illegally hack popular software programs. See Thomas Aff. ¶¶ 106-120; Ip Aff. ¶¶ 248-265.

**D. Direct Revenue Tolerated the Deceptive Acts of its Distributors**

92. Direct Revenue’s web of deceptive, stealth spyware distributions relies in large part on the fraudulent practices of its distributors (who Direct Revenue directly contracts to spread spyware) and subdistributors (who those distributors, in turn, hire to spread Direct Revenue’s spyware). While Direct Revenue always performs the actual installations of its programs to infected consumers from its own servers, see *supra* ¶ 24, these installations are often initiated by deceptive omissions and descriptions made by the company’s distributors and subdistributors.

93. Direct Revenue and its management have claimed that its distributors need not disclose its spyware to users when describing and advertising the “free” programs that are bundled with the spyware. Rather, they contend that it is sufficient to merely give the user some

opportunity to access Direct Revenue's EULA for its spyware programs – even when that license agreement is simply provided through a hyperlink and there is no other disclosure of the bundled spyware. As Vice-President for Distribution Christopher Dowhan has testified:

Dowhan: I have an understanding that they [distributors and subdistributors] have an obligation to give the consumer access to the EULA.

\* \* \*

Q: By access to the EULA, would a link to your EULA be sufficient, in your understanding?

Dowhan: In a layperson's understanding? A link would be access.

Exh. 20 (Dowhan Tr.) at 110-11. Indeed, this parallels Direct Revenue's own practice: in the OAG's tests of Direct Revenue's own bundled distributions (whether through proprietary websites or its own ActiveX advertisements), the only hint of the bundled spyware was given within a linked license agreement. See supra ¶¶ 42-52, 85-89.

94. On the other hand, Direct Revenue knew (or should have known) that many of its distributors and subdistributors were not even providing consumers this scant disclosure. As described infra, Direct Revenue's management had considerable notice about the clearly deceptive practices of its distributors and subdistributors through complaints, emails, public reports and other personal knowledge. See infra ¶¶ 136-160.

95. Even more remarkable, the company and its management had such ample notice despite their efforts to insulate themselves from knowledge of their distributors' and subdistributors' practices.

96. As a threshold matter, Direct Revenue made virtually no effort to ensure that its distributors obtained consent from consumers before installing its spyware. As one employee

candidly remarked to Joshua Abram, “We do not presently make much effort to assure that people are not getting our ads legitimately.” See Exh. 25 (email from M. Knox to J. Abram et al. dated April 7, 2005). Dowhan even testified that Direct Revenue’s “primary” means of policing its distributors was merely to require them to sign an Insertion Order. See Exh. 20 (Dowhan Tr.) at 97. (This Insertion Order included a provision at the bottom of the page incorporating by reference Direct Revenue’s “Standard Distribution Agreement,” which in turn required that consumers be “specifically informed” of the bundled spyware programs. See id. at 92-93.)

97. Although this was the company’s “primary” means of policing its distributors, Dowhan – who was responsible for the company’s distribution efforts – admitted that he had never even discussed the requirement of consent with any distributor prior to learning about the OAG’s investigation into the company:

Q: Did you have conversations with your distributors about these notice and consent provisions?

Dowhan: No. No distributor asked me about this provision or what it meant or anything along those lines.

Q: And you never proactively talked to a distributor about them?

Dowhan: No, I never.

Exh. 20 (Dowhan Tr.) at 94-95.

98. Dowhan further admitted that the company did not require that users be shown “short form disclosure,” i.e., up-front disclosure not contained within a license agreement, and did not require that distributors provide Direct Revenue with screen shots (or other information) evidencing disclosure of the bundled spyware. See Exh. 20 (Dowhan Tr.) at 81-85. Indeed, the

company often did not even ask distributors with what software they would be bundling Direct Revenue's spyware. See id. at 81-82.<sup>13</sup>

99. Furthermore, prior to September 27, 2005, Direct Revenue freely and unconditionally permitted its contracted distributors to subcontract out their role in initiating installation of Direct Revenue's spyware. See Exh. 24 (affidavit of Alan Murray). Distributors who subcontracted to parties who used deceptive means to distribute Direct Revenue's spyware programs were allowed to continue distribution with no more than a meek warning. See id. (noting that distributors Seedcorn, West Frontier, iDownload and Simpel Internet were allowed to continue to subcontract out distribution of Direct Revenue spyware, despite deceptive installations). Direct Revenue even allowed one partner, West Frontier, to continue distributing after three of its subdistributors were caught using security vulnerabilities to install Direct Revenue. See id.

100. So institutionalized was Direct Revenue's willful blindness that it tolerated its distributors' refusal to identify subdistributors – even when asked specifically about illegal practices. See Exh. 24 (affidavit of Alan Murray) (“Given this lack of knowledge, it was difficult for Direct Revenue to conduct direct policing of the subdistribution of its target software.”).

101. By the time Direct Revenue ceased distribution through parties who refused to identify subdistributors, the damage had been done: using the 22 companies it eventually terminated for refusing to identify subdistributors, or for specific instances of deceptive practices,

---

<sup>13</sup> After becoming aware of the OAG's investigation, Direct Revenue began requiring distributors to provide consumers with “short form” disclosure, and to provide Direct Revenue with information about the software that would bundle the spyware, as well as screen shots showing the disclosure that users received about the bundled spyware. See Exh. 20 (Dowhan Tr.) at 79-80.

Direct Revenue had already installed more than 87 million spyware programs.<sup>14</sup> Furthermore, the company continued to reinstall these programs if a user tried to remove the programs from his computer. See *infra* ¶¶ 127-128, 170; Exh. 6 (letter from N. Klausner to K. Dreifach *et al.* dated January 17, 2006) at 6-8.

102. Even worse, although Direct Revenue and its management plainly knew, and know, that millions of its spyware programs were illegally installed, it continues to display countless pop-up ads to those users, and continues to deliver stealth “updates” of its spyware programs. See *infra* ¶¶ 159-160.

**E. The Pernicious, Multiple Harms to Consumers From Downloading Direct Revenue’s Spyware**

103. In the words of Chief Technology Officer Daniel Doman, Direct Revenue’s spyware programs are “pretty spooky software.” See Exh. 28 (email from D. Doman to J. Cohen *et al.* dated April 20, 2005). Most obvious, the spyware bombards consumers with pop-ups ads. But it wreaks far greater havoc than that. For instance, the company’s programs open a permanent “backdoor” onto users’ computers, giving the company remote access from which it installs still more spyware, and does more mischief, as described below.

104. Compounding this intrusion, Direct Revenue has designed its spyware to be difficult, if not virtually impossible, to detect and remove. In fact, the spyware even reinstalls itself when removed by consumers savvy enough to detect and uninstall it.

---

<sup>14</sup> Direct Revenue did terminate two distributors – CDT and IST – prior to being served with an OAG subpoena. However, in both of those cases, the distributors were terminated because Direct Revenue suspected they were repeatedly uninstalling and then reinstalling Direct Revenue’s spyware in order to overcharge Direct Revenue for distribution. See, e.g., Exh. 26 (email from R. Hook to J. Abram, A. Murray *et al.* dated August 22, 2004); Exh. 27 (email from D. Doman to M. Simonsen dated September 16, 2004).

1. Incessant Pop-up Ads

105. The primary function of Direct Revenue's spyware is to show users a continuous stream of "pop-up" (and "pop-under") advertisements. Its software, once installed, permanently resides on users' computers. This allows Direct Revenue to send users a stream of pop-up ads every time they surf the internet, until they either figure out how to remove the program, or buy a new computer. In one test conducted by an OAG investigator, Direct Revenue popped up an ad for each of the twenty-three websites visited by the investigator. See Ip Aff. ¶¶ 19-20, 29, 35. In other tests, Direct Revenue even popped up advertisements when our investigators were not browsing the internet, and no Internet Explorer window was open. See, e.g., Thomas Aff. ¶ 135.

106. Direct Revenue's executives freely describe their advertising tactics as "hammering" or "abusing" consumers with pop-up ads. See Exh. 29 (email from D. Doman to K. Ryan et al. dated June 6, 2005) ("I have always believed that we are hammering users too often."); Exh. 30 (email from J. Abram to J. Stein dated March 7, 2005) (jokingly referring to "user abuse"). A small sampling of the numerous complaints the OAG has received about Direct Revenue's spyware shows the invasive nature of the programs:

- "I am inundated **with unwanted popups**"
- "Direct Revenue installed a program called 'A **Better Internet**' onto my computer without **my knowledge or permission**. It created a plethora of pop-up ads"
- "I too am infected with this 'virus.' It just popped up on my computer one day and now it will **not go** away. I never installed anything, **nor was** I asked to, it seems to have **installed** itself. It is **sucking** up my internet connection, as well as our network connection and has **lost our organization money in technical** consulting fees to try and figure out **what** happened to our internet connection"
- "It installed so many pop up ads that **I couldn't continue** my work. My system crashed and I lost all my work"

- “Because of having been quite obviously and unconsciously tricked into downloading this unsolicited file, I now receive pop-up advertisements as often as every few seconds. . . . This unwanted program wastes literally hours of my time, and has also slowed down my computer and twice nearly crashed it”
- “This malware, worm, whatever . . . has taken over my computer, constantly interrupting work or research with pop-up after pop-up”
- “This company maliciously and secretly download its software onto my computer. It pops up ALL the time and it cannot be uninstalled the way programs can be uninstalled. It has ruined my computer and I still cannot remove it”
- “The incessant popups – whether I’m online or not make my computer virtually unusable”
- “Without my consent they [Direct Revenue] were able to infect my computer with their malicious adware and I have spent the last week trying in vain to remove it. I am at the point where I am willing to do most anything to get this thing off my computer, short of a full system format and reinstall. I own a small computer retail and repair company and do most of my billing and sales from this computer. Direct Revenue’s Software has basically brought my work to a stand still with their constant popups.”
- “Direct Revenue installed malware on my computer without my knowledge. This malware changed my registry [and] causes a barrage of popup ads”
- “It makes pop-ups appear whenever I try to use my browser and I can not stop them from popping up with a pop-up blocker”
- “A Better Internet somehow installed spyware on my PC which bombarded me with pop up windows – at times even when working in Excel or Word. The popups were so prolific it became a serious interruption in my work flow.”

See Exh. 31 (sampling of complaints to the Office of the New York Attorney General); see also Exh. 32 (sampling of additional complaints to the Office of the New York Attorney General).

107. So intrusive was its spyware that even Direct Revenue employees and clients complained to management about the frequency of ads shown. See Exh. 27 (email from G. Walter to K. Ryan dated June 6, 2005) (“I got at least 30 ads today from Aurora . . . sometimes

back to back within a minute. . . . My computer crashed 4 times and I noticed that after I turn it back on I get a lot of ads in the first 20 minutes . . . .”); id. (“One of the Monster[.com] media buyers had basically the same experience with Aurora and started asking questions.”).

108. In response to such complaints about ad bombardment, Direct Revenue management experimented with “taking the ad spacing to 2 minutes apart.” But senior management rejected the change after noticing a 15% drop in revenue. See Exh. 33 (email from R. Hook to J. Engroff et al. dated June 8, 2005) (complaining about “painful experiment” of reducing ad timing to once every two minutes); Exh. 34 (email from D. Kee to D. Doman et al. dated June 16, 2005) (“Rod [Hook] experimented with changing the minimum ad time from 45 seconds to 2 minutes but he said our revenue dropped significantly. . . . He changed the minimum ad time back to 45 seconds.”).

109. Direct Revenue generates its ads through a sophisticated, stealth tracking system, monitoring the websites that users visit, and the text users enter into web forms, such as searches on Google or Yahoo!. See Exh. 24 at ¶¶ 9-11. (affidavit of Alan Murray). This information is sent back to and stored on Direct Revenue servers – along with the user’s IP address, Machine ID, Windows ID and a list of processes running on the user’s computer. See id. Earlier versions of Direct Revenue’s spyware, such as “VX2,” “TPS108” and “IEHelper,” transmitted additional personally identifiable information back to Direct Revenue, including first and last name, mailing addresses and email addresses. See id.

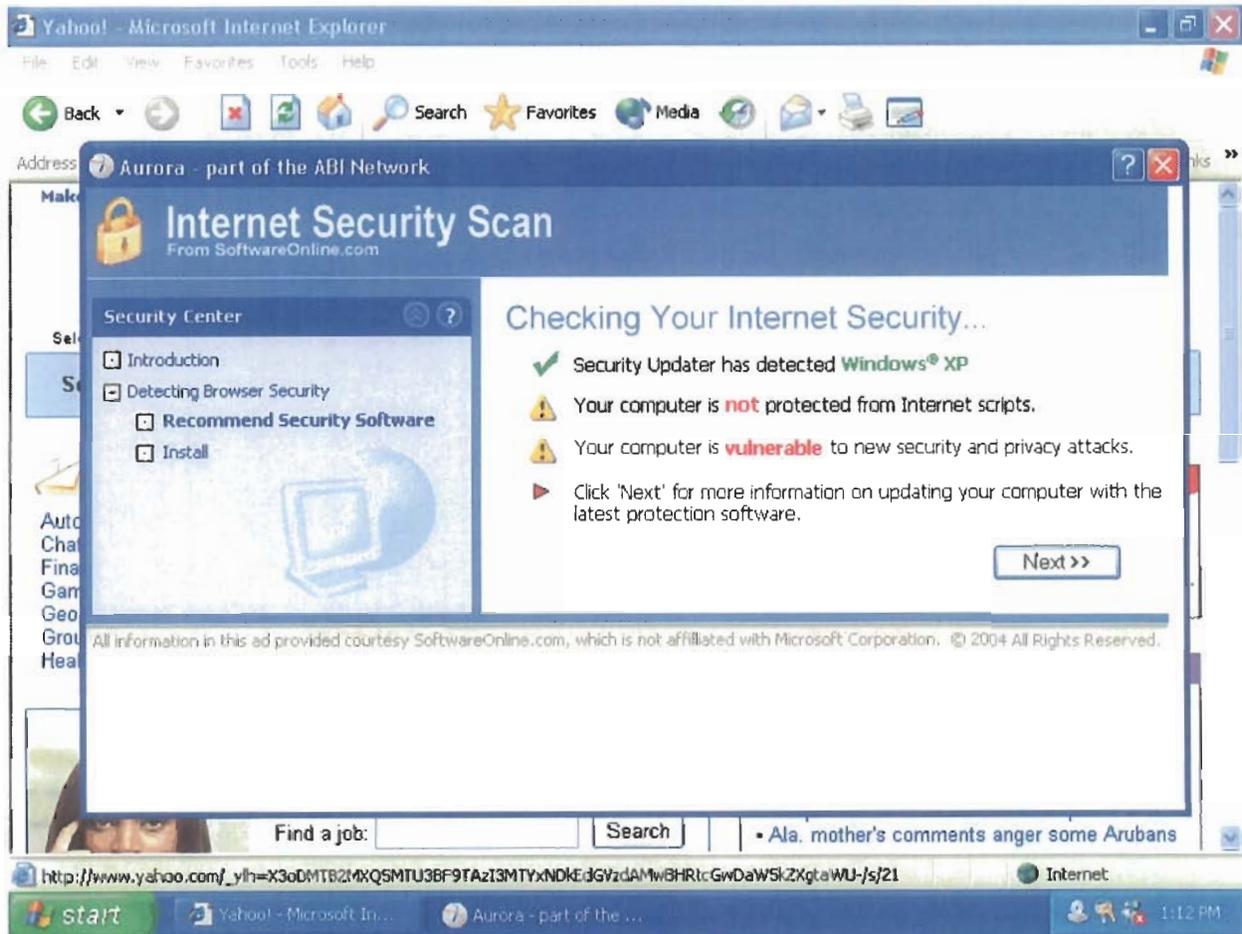
110. While many of the ads shown by Direct Revenue spyware are dubious offers for, e.g., offshore gambling websites and “free laptops,” see Thomas Aff. ¶ 18, mainstream companies have also advertised through Direct Revenue’s spyware. In the OAG’s tests,

investigators documented numerous ads for prominent companies such as Priceline, Cingular, Monster.com, JPMorgan Chase and United Airlines. See, e.g., Ip Aff. ¶ 20, 29, 97, 265; Thomas Aff. ¶¶ 37, 57.

111. Some advertisements, ironic as they are deceptive, attempt to fool consumers into installing “anti-spyware” programs – often imitating security warnings or updates generated by the user’s own computer. (These deceptive ads conveniently omit that these “anti-spyware” programs will not remove the spyware that Direct Revenue already has placed on their computers.) See, e.g., Exh. 35 (email from J. Stein to J. Abram, A. Murray, D. Kaufman et al. dated March 7, 2005) (reporting new advertising campaign for “Spyware Nuker” program).

112. One ad repeatedly shown to our investigators by Direct Revenue’s spyware, for instance, mimicked a Windows “Internet Security Update,” in an effort to fool users into installing anti-spyware software from SoftwareOnline.com. See, e.g., Thomas Aff. ¶¶ 97, 105, 119; Ip Aff. ¶ 109; Screen Shot No. 13 below. This fake security alert informed the user that it had detected Windows XP running on the user’s computer, but warned that the user lacked “the latest security updates” and “is vulnerable to new security and privacy attacks.” See id. (emphasis in original). The ad also featured a link instructing users to install a “Recommended Security Update.” See id.

**SCREEN SHOT NO. 13**



113. Despite long-standing recognition within the company that this and other anti-spyware ads were inherently deceptive, see, e.g., Exh. 36 (email from J. Engroff to J. Abram, A. Murray et al. dated April 26, 2005); Exh. 37 (email from C. Dowhan to J. Abram, A. Murray et al. dated July 8, 2004), Direct Revenue continued to display these advertisements to infected users. As Josh Engroff, Direct Revenue's Vice President for Advertising Sales, summarized: "As most of you know, there has been a long-running debate about Software Online, and the decision each time has been not to shut them down . . . . Software Online is a huge spender and

have been running their ads for a long time on our network.” See Exh. 38 (email from J. Engroff to J. Abram, A. Murray, D. Kaufman, R. Hook et al. dated January 17, 2005) (rejecting plea from Direct Revenue’s Chief Technology Officer Dan Doman that “These campaigns should be turned off ASAP. We should never run this sort of thing.”).

114. Indeed, an audit by Direct Revenue’s ad-selling division, Soho Digital, revealed that Software Online was the company’s single most profitable advertisement. See Exh. 39 (email from J. Engroff to A. Murray et al. dated April 27, 2005); see also Exh. 40 (email from J. Engroff to J. Stein et al. dated March 7, 2005) (referring to Software Online and similar anti-spyware and anti-spam advertisements: “I think we’ve all agreed that these are not the most desirable campaigns in the world, but that we are going to max the hell out of them during March and April”). See also Exh. 41 (email from D. Kaufman to J. Abram, A. Murray, R. Hook et al. dated August 16, 2005) (reporting that new distribution partner Kazaa was “most concerned about some of our ads that they claim (probably correctly) are purposefully confusing to the user”).<sup>15</sup>

115. In the OAG’s tests of Direct Revenue’s ad-serving spyware programs, investigators encountered other advertisements for computer registry cleaners, anti-spyware programs and anti-virus protection. See, e.g., Thomas Aff. ¶¶ 17, 36, 66, 79, 104, 120; Ip Aff. ¶¶ 19-20, 29, 35, 96, 109, 146. An internal analysis of Direct Revenue’s advertising base conducted in June 2005 determined that such “Downmarket Direct Marketer” advertisements have accounted for approximately 37% of the company’s advertising revenue. See Exh. 43

---

<sup>15</sup> Casale Media — which paid Direct Revenue to run a similar, misleading anti-spyware ad to infected computers — ceased its campaign in May 2005 due to liability concerns. See Exh. 42 (email from W. Chavez to J. Abram et al. dated May 17, 2005).

(email from W. Chavez to J. Abram, A. Murray *et al.* dated June 6, 2005).

2. Prevents Detection and Removal

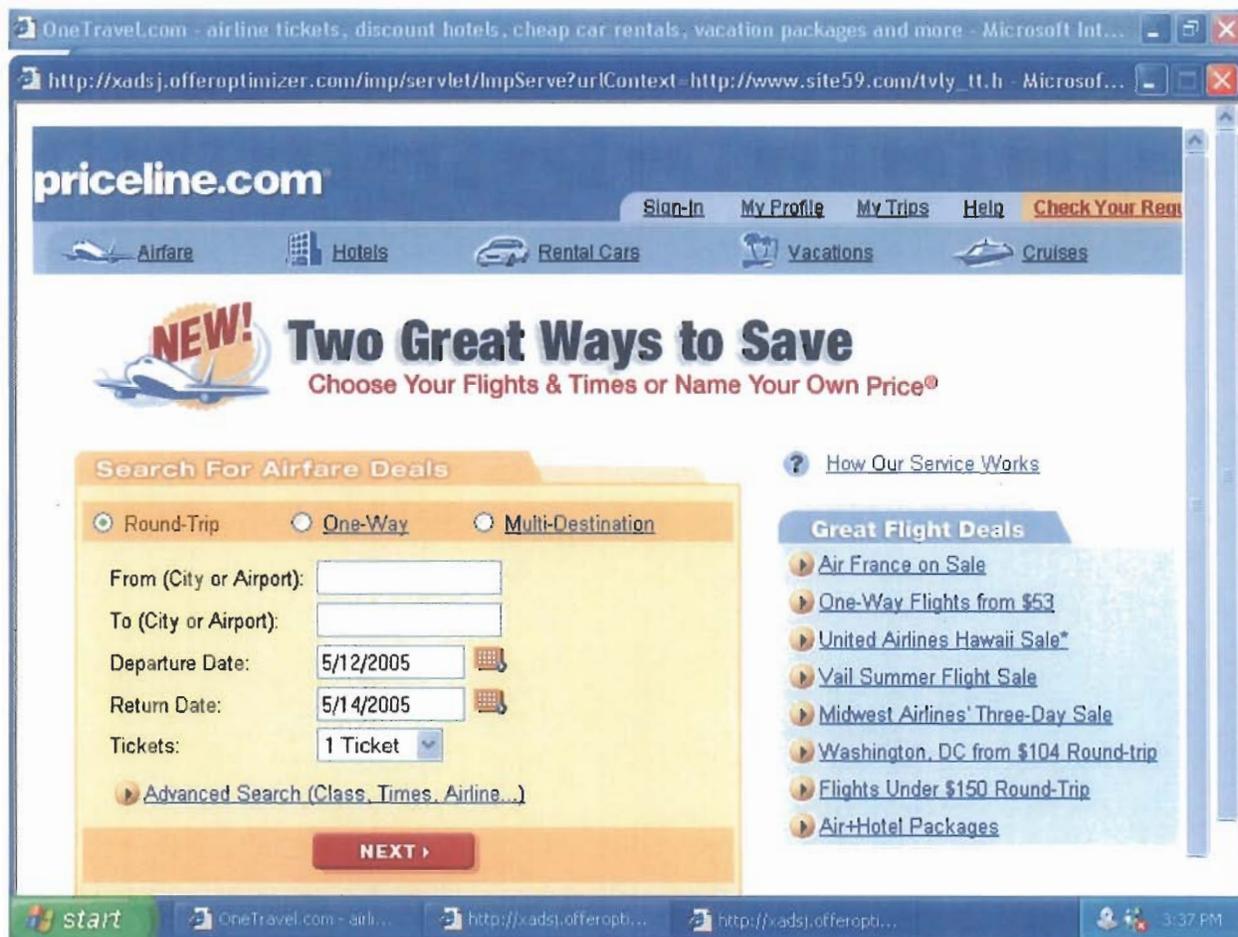
116. Greatly compounding damage to users, Direct Revenue designs its spyware to be virtually impossible to detect and remove. While most software programs are installed in the “Program Files” folder on users’ hard drives, Direct Revenue scatters its files across users’ computers, in unlikely locations such as the “Windows,” “System32,” and “Inf” folders typically reserved for Microsoft Windows files. *See, e.g.*, Thomas Aff. ¶¶ 33, 59. Direct Revenue gives these files randomly generated names such as “ucpvyttbvt” and “hhqbijwqy,” and even ascribes to these hidden files false modification dates to make it appear as if they had been created much earlier. *See id.* ¶¶ 59, 70, 84, 99, 116, 137; Rivela Aff. ¶¶ 8-9, 30-31, 51-52.

117. Direct Revenue also changes the names of its files and processes on a regular basis, in a further effort to frustrate users seeking to identify Direct Revenue’s programs. *See, e.g.*, Exh. 44 (email from R. Hook to J. Abram, A. Murray, D. Kaufman *et al.* dated March 8, 2005) (questioning whether distributors would be willing to bundle Direct Revenue’s “incredibly polymorphic” spyware); Thomas Aff. ¶¶ 59, 70, 84, 99, 116, 137. All of these elements are part of Direct Revenue’s self-titled “obfuscation process,” to which the company has devoted tremendous resources and manpower. *See, e.g.*, Exh. 45 (email from B. May to A. Chapell *et al.* dated June 17, 2005). In fact, the company even had an entire department named “Dark Arts” which was tasked to “increase stealth” for Direct Revenue’s spyware components. *See* Exh. 46 (email from R. Ross to J. Abram dated May 5, 2005).

118. For most of the company’s history, Direct Revenue’s pop-up ads did not identify Direct Revenue as the ads’ source. *See* Exh. 47 (email from J. Hook to J. Abram, A. Murray, D.

Kaufman dated January 20, 2004) (Direct Revenue business plan, showing representative ads). Instead, the header for the ad simply contained the name of the ad network placing the ad, or simply a string of gibberish. See Screen Shot No. 14, below. As a result, users had no way of knowing that Direct Revenue was responsible for generating the pop-up ad. Most users would likely assume that the pop-up ads were simply being generated by the websites they visited. Because these ads often took up the entire screen, a casual computer user might not even notice that the window in front of him was not the site he requested, but actually an advertisement placed there by Direct Revenue's spyware program.

**SCREEN SHOT NO. 14**



Direct Revenue began using primarily “branded” ads in the summer of 2005, but has frequently switched brands and logos, presumably due to the negative publicity its programs have received. Direct Revenue most recently scuttled its infamous “Aurora” brand and logo in September 2005, in favor of the name “Best Offers” and a new logo. See Exh. 48 (Direct Revenue press release). Other names that Direct Revenue has given its spyware over its short history include “Solid Peer,” “Ceres,” “VX2,” “TPS108,” “Pynix,” “IEHelper,” “LocalNRD,” “MSView,”

“BetterInternet,” “OfferOptimizer” and “Twaintec.” See Exh. 24 (affidavit of Alan Murray).

119. If detecting Direct Revenue’s spyware on a computer is difficult, removing it is harder still. First, Direct Revenue designs its spyware so that when the user uninstalls the program with which the spyware was bundled (e.g., the IEPrivacy security program, or FreePhone telephony program), Direct Revenue’s pop-up program (and any other spyware program Direct Revenue added subsequently) remain behind, fully operational. See Ip Aff. ¶ 25-29.

120. Direct Revenue also fails to provide a stand-alone mechanism for users to uninstall its spyware, such as an identifiable “uninstall” file accessible through the “All Programs” list or an easily located program file. See, e.g., Ip Aff. ¶ 17. Such uninstall functions are common in the software industry. See Exh. 49 (FTC Staff Report, Monitoring Software On Your PC: Spyware, Adware and Other Software, March 2005, p. 7) (“FTC Report”) (discussing problem of spyware programs that “cannot be removed using the Add/Remove Programs function and do not provide their own uninstaller,” and citing testimony).

121. Most remarkably, for much of the company’s history, Direct Revenue did not list its spyware programs in Microsoft’s “Add/Remove Programs” utility. See Ip Aff. ¶¶ 21, 162, 219, 247, 257; Thomas Aff. ¶¶ 20, 35, 82; see also Exh. 13 (email from C. Dowhan to R. Khan et al. dated July 14, 2004) (“We don’t use any add/remove programs entry for our stuff except for a few specific ‘polite’ installs we do from the <http://www.abetterinternet.com> site for investors, etc.”). The “Add/Remove” feature, located in the computer’s “Control Panel,” is easily accessed from the Start Menu and is by far the most common mechanism by which consumers remove

unwanted programs from their computers. See Exh. 49 (FTC Report).<sup>16</sup>

122. In order to maintain the fiction that users could remove its spyware, Direct Revenue set up a special website, called MyPCTuneUp.com, to host an “uninstall” program that users could download to remove the company’s spyware. This site was designed to be the only way users could remove Direct Revenue spyware from their computers. See Exh. 51 (email from C. Dowhan to J. Abram dated June 8, 2005) (stating “our strategy has been to make the ad client as hard as possible to uninstall through any means other than MyPCTuneUp”).

123. How users were supposed to find or learn about MyPCTuneUp.com, however, remains a mystery. Even the most diligent and savvy computer user would be unlikely to discover the website. Searches by an OAG investigator on common search engines for terms such as “Aurora,” “Aurora Spyware,” “Ceres,” and “Direct Revenue” did not generate any entries for MyPCTuneUp.com. See Ip Aff. ¶¶ 266-270. Even in its internal investigations, the OAG learned of this website and its uninstall program only after dozens of hours of reading internet message boards discussing the removal of Direct Revenue’s spyware programs.

124. Direct Revenue and its principals knew that few users were likely to find MyPCTuneUp.com. See Exh. 52 (email from D. Kaufman to J. Abram, A. Murray, R. Hook et al. dated February 2, 2005) (“my own personal vote would be that we have NO uninstall (other than a user somehow finding his way to mypctuneup)”); infra ¶¶ 162-167. They also knew that users were unlikely to trust Direct Revenue enough to consent to willingly install purported

---

<sup>16</sup> Direct Revenue did not begin offering Add/Remove entries for most of its spyware programs until at least May 2005, when it learned of the OAG’s investigation into its practices. See infra ¶¶ 160-169; Exh. 51 (email from C. Dowhan to J. Abram dated June 8, 2005).

“uninstallation software” from the very company that snuck spyware onto their computers in the first place. See infra ¶ 166. Furthermore, they knew that MyPCTuneUp often would not work, given the highly sophisticated, constantly changing nature of Direct Revenue’s spyware. See Exh 135 (email from T. Davis to D. Doman et al., dated June 2, 2005) (“The email [complaint about MyPCTuneUp] below from one of our frustrated users illustrates another of the ‘costs’ of stickiness [the ability to stay on a user’s computer] in addition to the engineering itself. As we get more sticky, we also have more moving parts with more possible failure points.”).

125. Indeed, the company knew MyPCTuneUp would not work at all if the user had a common firewall in place on his system, such as from Symantec or McAfee – thus making their spyware essentially non-removable for millions of users. See Exh. 53 (email from D. Doman to R. Minassian dated May 26, 2005).<sup>17</sup>

126. In the OAG’s tests of MyPCTuneUp.com, Direct Revenue’s uninstaller often left numerous files behind – and in some cases failed to function at all. See Thomas Aff. ¶¶ 38-47; Rivela Aff. ¶¶ 15-21, 37-43.

127. Direct Revenue designed its spyware to resist and evade any other effort to remove Direct Revenue’s spyware programs by conventional methods, such as manual deletion or using anti-spyware software. One of the many tactics used by Direct Revenue to frustrate removal is to install numerous “lifeboats” – small programs that monitor the status of the primary spyware program, and reinstall it if the spyware is deleted by the user. See, e.g., Exh. 55 (email

---

<sup>17</sup> Earlier versions of MyPCTuneUp were even more burdensome to consumers. Users had to visit the MyPCTuneUp site, enter an email address and name, and then wait for Direct Revenue to email back a link that would allegedly uninstall the unwanted software. See Exh. 54 (email from M. Simonsen to A. Konanykin dated August 18, 2004).

from C. Dowhan to D. Doman dated July 9, 2004) (also discussing “obfuscation” of lifeboats from users); Exh. 56 (email from D. Doman to J. Abram, A. Murray et al. dated August 31, 2004) (discussing “stubby” and “poller” lifeboats that reinstall Direct Revenue spyware after deletion). Direct Revenue has even held regular “Anti-Virus/Anti-Spyware Meetings” designed to pinpoint which anti-spyware software programs were identifying and removing Direct Revenue spyware, and to devise new means to avoid such identification and removal. See, e.g., Exh. 57 (email from C. Dowhan to R. Hook et al. dated June 17, 2005); Exh. 58 (email from J. Rush to R. Hook et al. dated June 17, 2005) (sending weekly scan of whether major anti-virus and anti-spyware programs were able to detect and remove Direct Revenue spyware). See also Exh. 59 (email from D. Doman to B. May et al. dated June 2, 2005) (expressing dismay that user was able to remove Direct Revenue spyware after running Ewido security software in Windows “Safe Mode”).

128. In tests conducted by OAG investigators, attempts to remove Direct Revenue spyware either manually or using common anti-spyware programs (such as Lavasoft’s Ad-aware and Safer Networking’s Spybot – Search and Destroy) were unsuccessful; every time, Direct Revenue’s spyware reinstalled itself on our test computers. See, e.g., Ip Aff. ¶¶ 24-36; 49-50. In one representative test, an OAG investigator, after failing to locate an entry for Aurora in Add/Remove, tried to remove the program five times in succession using the common spyware removal program Ad-aware. See Ip Aff. ¶ 24-36. In each instance, Direct Revenue’s spyware silently reinstalled itself onto the test computer’s hard drive and continued to send pop-up advertisements. See id.

### 3. Installs Other Spyware Programs and Updates Existing Spyware

129. In addition to its ad-serving, user-tracking functionality, Direct Revenue's spyware has installed onto users' computers hidden "updater" programs which give Direct Revenue permanent remote access to all infected computers. Direct Revenue constantly uses these updater programs to add still more spyware onto users' computers, without any notice or consent, and to bury its spyware even deeper into a user's computer. See Exh. 24 (affidavit of Alan Murray).

130. Direct Revenue has made use of these updater functions on a daily basis, regularly adding new versions of its own programs – as well as additional spyware programs – to users' computers. See Exh. 60 (email from C. Dowhan to D. Doman et al., dated January 21, 2005) (describing adding new versions of pop-up software and other third-party spyware programs onto users' computers as "normal daily maintenance"). Direct Revenue's schedules of historical "updates" show millions upon millions of instances where Direct Revenue remotely updated infected computers with new spyware. See Exh. 2 at Schedule 3, Schedule 6.

131. For instance, through this stealth "updater" feature, Direct Revenue has added to millions of already infected computers a "404 redirect program." This program effectively takes control of users' browsers, redirecting users to Direct Revenue websites.<sup>18</sup> One "404 redirect"

---

<sup>18</sup> Specifically, whenever a user requests an incorrect or non-existent web address, Direct Revenue's redirect spyware program sends him instead to a Direct Revenue search page. See Rivela Aff. ¶ 57. "404" refers to the "404 Error Page" that Internet Explorer page traditionally presented to users who had entered erroneous or mistyped addresses. The program also installs Direct Revenue's search page as the default search engine in Internet Explorer. Thus, when a user clicks the "Search" button on an Internet Explorer toolbar, he is redirected to Direct Revenue's search page. See Exh. 66 (email from M. Stanghed to J. Abram dated April 8, 2005).

program, authored by Direct Revenue's partner Walnut Ventures, was remotely installed by Direct Revenue to over 17 million users. See Exh. 2 at Schedule 6. Direct Revenue even remotely added other pop-up ad programs (such as TopMoxie's "Moe Money" program) and programs that placed additional toolbars and buttons onto users' Internet Explorer interface. See id. at Schedule 6 (describing over 10 million remote installations of TopMoxie's software); id. at Schedule 3 (discussing remote installations of "Microbuddy" toolbar).<sup>19</sup>

132. Direct Revenue gave consumers no notice of any of these silent updates. See, e.g., Exh. 62 (email from R. Hook to C. Nardone et al. dated December 20, 2004) (discussing silently adding other spyware programs to existing users); Exh. 63 (email from M. Stanghed to C. Dowhan et al. dated October 22, 2004) (same).

133. In addition to installing other spyware programs, Direct Revenue regularly uses its "updater" functions to silently install increasingly sophisticated (i.e., harder to detect and remove) versions of its own pop-up ad programs. These "improved" versions employ Direct Revenue's latest schemes to evade detection, as well as new lifeboats to reinstall the spyware if a user later manages to delete it. See Exh. 60 (email from R. Hook to J. Abram, A. Murray, D.

---

Direct Revenue profits from this hijack of users' computers whenever users arriving at the redirected page use the search engine or suggested links available on the page. Yahoo! provides Direct Revenue with the search capability and suggested links, and the two companies split the proceeds. See Exh. 61 (email from M. Stanghed to J. Abram, A. Murray, D. Kaufman et al. dated June 2, 2005). The generic looking page to which users are redirected makes no reference whatsoever to Direct Revenue, or to any spyware program that sent the user to the page. See Rivela Aff. ¶ 58.

<sup>19</sup> For much of the company's history, these supplemental spyware programs had no process for removal or uninstallation – even through MyPCTuneUp. See Exh. 13 (email from R. Khan to C. Dowhan et al. dated July 14, 2004) (stating that 404 redirect program "currently has no real uninstall process and definitely does not create any add/remove programs entry. But we don't want anyone to uninstall anything if we can help it").

Kaufman et al. dated January 21, 2005). Newer versions also typically include Direct Revenue's latest "torpedos" – small programs designed to delete or disable competing spyware programs. See id.; Exh. 64 (email from C. Dowhan to J. Abram, A. Murray, D. Kaufman, R. Hook et al. dated November 12, 2004) (discussing distribution of torpedos to attack competing BullsEye, Dyfuca and WinTools spyware programs).<sup>20</sup>

134. In effect, Direct Revenue has long treated each user's hard drive as the company's personal playground once users are infected with its spyware. The installation of additional spyware and more sophisticated versions of existing spyware necessarily degrades computer performance and slows other network or internet communications. Nevertheless, Direct Revenue blithely commandeers the resources of infected computers to further secure its own spyware, and to add the spyware of its partners. Predictably, consumers are given no notice about these constant "updates."

**F. Abrams, Murray, Kaufman and Hook Participated In And Were Aware of Direct Revenue's Unlawful Practices**

135. In October 2002, Abrams, Murray, Kaufman and Hook (collectively the "individual respondents") founded Direct Revenue.<sup>21</sup> Since that time, they have overseen and directed Direct Revenue's business operations.

---

<sup>20</sup> In order to disable competing spyware programs, Direct Revenue has gone so far as to alter users' security settings without any notice or consent. See, e.g., Exh. 65 (email from D. Doman to J. Abram, A. Murray, D. Kaufman, R. Hook et al. dated December 21, 2004) (acknowledging "This is a MAJOR security no-no. I guess we have to bite the bullet.").

<sup>21</sup> Previously, the individual respondents had founded another adware company called Dash.com and a spam/data mining business named True Data. See Exh. 67 (email from J. Abram to A. Murray dated October 24, 2002) (discussing rates for "email blasting"); Exh. 68 (email from H. Giles to A. Murray, R. Hook et al. dated October 23, 2002) (discussing "mining" of personally-identifiable information by True Data); Exhs. 69 & 70 (sample spam complaints).

136. These individual respondents built a business model based on wide-scale fraud. Spyware has been the company's primary (if not only) line of business throughout its existence.

137. Internal email and correspondence show that the individual respondents knew of, participated in, and encouraged Direct Revenue's non-consensual spyware downloads. Likewise, each was involved in the decision to make this stealth spyware very difficult for users to discover on their computer, and to uninstall. Furthermore, each knew and participated in Direct Revenue's decisions to bombard users with misleading ads, and use stealth "updater" functions to upload still more, hidden, spyware programs.

138. As then-Chief Technology Officer Daniel Doman warned the individual respondents in May 2005, "(1) Users don't know how they got our software (this is both upgrade and recent install . . .). (2) Users say that they are getting so many ads that it is annoying them." See Exh. 71 (email from D. Doman to J. Abram, A. Murray, D. Kaufman, R. Hook et al., dated May 27, 2005) (ellipsis in original).

1. The Individual Respondents Knew that Direct Revenue Was Installing its Spyware onto Users' Computers Without Notice or Consent

139. The individual respondents knew Direct Revenue's bait-and-switch practice of bundling spyware with other software programs was inherently deceptive. As Tom Phillips, a partner from an outside investment firm, commented early on, because "the entry to the desktop is accomplished through a bundled download . . . the consumer is not always aware of what is being delivered through that bundle." See Exh. 72 (email from J. Abram to A. Murray dated March 1, 2004) (forwarding analysis of "Consumer Legitimacy"). Given the lengths to which Direct Revenue went to bury notice of the bundled spyware programs, Mr. Phillips' comment is a

spectacular understatement.

140. Each of the individual respondents understood that when Direct Revenue distributed its spyware “bundled” with another program, the sole reference (if any) to Direct Revenue or its hidden spyware was hidden within a linked EULA or “Consumer Policy Agreement” where the average consumer would not see it. See, e.g., Exh. 73 (email from C. Dowhan to J. Abram, A. Murray, D. Kaufman, R. Hook dated April 12, 2004) (describing Direct Revenue ActiveX “advertisement” that omitted mention of bundled spyware). They also knew that Direct Revenue’s distributors were (at best) using the same deceptive practice of hiding notice in a license agreement that consumers were not required to view. See, e.g., Exh. 74 (email from M. Stanghed to J. Abram, A. Murray, R. Hook et al. dated February 22, 2004) (forwarding criticism of Direct Revenue distribution bundle that included notice of spyware only at end of license agreement); Exh. 75 (email from C. Dowhan to J. Abram, A. Murray, D. Kaufman, R. Hook et al. dated June 16, 2005) (defending practice of providing notice of Direct Revenue programs solely through link in another program’s EULA); see also Exh. 76 (email from M. Simonsen to J. Abram et al. dated March 24, 2004) (responding to distributor worried about legality of Direct Revenue’s practices: “We state what they’re downloading in terms and conditions.”); Exh. 77 (email from W. Miller to J. Abram et al. dated May 1, 2005) (describing download process where users are only shown link to Direct Revenue EULA on one installation screen).

141. The individual respondents also knew that users whose security settings were not sufficiently high would not receive any notice for distribution through ActiveX mechanisms – the majority of the company’s installs. See Exh. 78 (email from J. Abram to A. Murray, D. Kaufman

et al. dated March 2, 2004) (noting that “someone might leave their browser on a page [hosting a Direct Revenue ActiveX advertisement] with low security setting on their machine causing us to automatically download”).

142. Yet the individual respondents could not have believed that notice within a linked license agreement constituted meaningful disclosure. In discussing whether Direct Revenue’s policy complied with Google’s requirement that consumers be “conspicuously notified” of bundled adware, the company’s Vice-President for Distribution stated: “Our EULA definitely explains to the user that they are getting adware in exchange for a utility . . . but I’m not sure about the ‘conspicuously notified’ part of their terms.” See Exh. 79 (email from C. Dowhan to A. Murray et al. dated April 12, 2005). Even more revealing, as Abram boasted to a potential distributor as recently as April of 2005:

We have a very stealthy version of our adware product which we’re happy to give u. The little pieces — like the 404 [redirect] and the microbuddy [toolbar] are custom integrations. Don’t worry. If we do a deal — and a build together — these will not be caught.

See Exh. 80 (email from J. Abram to W. Sager, dated April 26, 2005).

The Individual Respondents Were Aware  
That the Company Was Using Untrustworthy Distribution Partners

143. The individual respondents knew (or should have known) that many of the company’s distributors would not even give consumers access to its End User License Agreement. Each of the individual respondents knew that Direct Revenue used disreputable third parties to distribute its spyware programs across the internet. See, e.g., Exh. 81 (email from J. Abram to A. Murray, R. Hook et al. dated February 9, 2004) (discussing intention to “reach further into the bowels of the internet” for distribution partners); see also Exh. 82 (email from D.

Doman to J. Abram, A. Murray, D. Kaufman et al., dated May 5, 2005) (“To be perfectly honest, we DO HAVE some ad clients that were acquired through second rate distributors and possibly via suspicious mechanisms).

144. The individual respondents knew that Direct Revenue’s distributors were installing numerous other spyware programs in addition to Direct Revenue’s, thus further obfuscating users’ ability to determine what programs were installed, by whom and at what point in time. For instance, Abram candidly admitted to Murray in early 2004 that distributor Mindset Interactive was bundling fourteen spyware programs in addition to Direct Revenue’s pop-up program, noting: “It’s ugly out there.” See, e.g., Exh. 83 (email from J. Abram to A. Murray dated January 27, 2004); see also Exh. 12 (email from M. Stanghed to J. Abram, A. Murray, D. Kaufman, R. Hook dated April 27, 2005) (noting that distributor Skyhorn was likely installing Direct Revenue through “browser exploit [vulnerability] with 10 other people [e.g., other spyware companies] or the like”); Exh. 84 (email from C. Dowhan to J. Abram et al., dated March 1, 2005) (noting that Direct Revenue was being bundled with notorious spyware programs CoolWebSearch and EliteBar).

145. The individual respondents knew no consumer would willingly agree to install ten to fifteen spyware programs on their computer in exchange for a free screensaver – and certainly not in exchange for an undefined “browser enhancement.” Indeed, they freely admitted that there was no above-board value exchange with consumers. See Exh. 85 (email from D. Doman to J. Abram et al., dated May 4, 2005) (“We still need to establish a fair exchange of value with the software that we bundle with . . . .”); Exh. 86 (email from J. Abram to R. Ross dated May 24, 2005) (“With the exception of p2p [file trading software], none of our products – nor those of our

competitors – has the slightest traction with consumers”).

146. The individual respondents even ignored detailed complaints about particular distributors. For example, although Abram had been informed repeatedly that Pacerd was using clearly deceptive methods to distribute the company’s spyware, he consistently refused to investigate or suspend Pacerd. On April 4, 2005, for instance, Direct Revenue employees forwarded to Abram and Hook an article excoriating Direct Revenue for installing its spyware through the abusive advertisements described supra, ¶¶ 75-84. See Exh. 87 (email from D. Doman to J. Abram dated April 4, 2005). Two months later, a complaint from anti-spyware activist Ben Edelman was forwarded to Abram and others, again documenting how Pacerd installed Direct Revenue using deceptive practices. See Exh. 88 (email from C. Dowhan to J. Abram et al. dated June 7, 2005). Doman even confirmed, “We are doing exactly what they [Edelman] are accusing us of doing.” See Exh. 89 (email from D. Doman to J.P. Maheu dated June 13, 2005).

147. Nevertheless, when OAG investigators tested Pacerd’s installs in May, June, August and September of 2005, Direct Revenue was still using that company to install its spyware programs without notice to consumers. See Ip Aff. ¶¶ 166-177; Thomas Aff. ¶¶ 60-86; Rivela Aff. ¶¶ 3-12, 22-33, 44-54. Similarly, Abram flatly ignored complaints about distribution tactics used by its distributor Optisoft in bundling its spyware with the FasterXP program. See Exh. 10.

148. Direct Revenue and the individual respondents did not have to rely on third parties to notify consumers and obtain consent before installing Direct Revenue adware. As noted supra at ¶ 24, Direct Revenue’s distributors and subdistributors only install a small stub

file onto users' computers; Direct Revenue itself uploads and installs the actual spyware. Thus, Direct Revenue always had the option to notify consumers of the spyware at the actual moment of installation. As Chris Dowhan stated:

Our only record that [distributors] have complied [with notice and consent obligation] is the fact that a download and install occurred – we have no explicit knowledge of an opt-in because we don't require acceptance of terms during install itself, only during the download. Also, we do not monitor their live distribution to see that they are in compliance.

See Exh. 73 (email from C. Dowhan to J. Abram, A. Murray, D. Kaufman, R. Hook et al., dated April 12, 2004). Although Dowhan suggested the possibility of Direct Revenue itself providing some degree of notice during installation, the practice was not adopted. See id.

The Individual Respondents Were Aware of  
Widespread Criticism and Countless Complaints

149. Each of the individual respondents knew of the litany of complaints to Direct Revenue from angry, confused users. The individual respondents began receiving regular complaints from bewildered users even before they had incorporated Direct Revenue in November 2002. See Exh. 90 (email from D. Kaufman to A. Murray dated October 16, 2002) (forwarding complaint from user about early spyware variant); Exh. 91 (email from D. Kaufman to A. Murray dated October 16, 2002) (noting he was personally receiving “one of these [complaints] a day”).

150. These early complaints plainly indicated that consumers were not willingly downloading and installing Direct Revenue's spyware programs. One typical complaint to Kaufman read:

I have recently found a file called SentryStub.exe [an early Direct Revenue variant] on my machine. It has been placed there without my consent, and I resent this intrusion of my privacy. I've spent quite some time trying to find out what this file is and where it came from. I am not alone, there are a heap of really pissed off and concerned people trying to get details as well.

Your name and address is posted as [the] most likely originator of this problem, and I urge you and your associates to desist with the slimy ways of getting this file into our systems. If you have a legitimate and honorable reason to distribute this file, one would expect those reasons to be stated up front, and for permission to be asked.

See id.

151. This complaint is tame compared to others the individual respondents received on a regular basis. Yet Direct Revenue's management became so enured to users' wrath that they mockingly forwarded to each other some of the more creative death threats against them and their families. See, e.g., Exh. 92 (email from D. Doman to A. Murray et al., dated June 15, 2005).

152. The individual respondents personally received (at least) hundreds of these complaints about the company's practices over the past four years. Kaufman received the earliest complaints because many of Direct Revenue's web domains were registered to his name. See, e.g., Exhs. 91 & 92. In 2003 and 2004, complaints were sent to a Yahoo! account of Murray specifically set up to field criticism from angry users. See, e.g., Exh. 93 (sampling of representative complaints). In 2005, complaints were automatically forwarded to Abram's email address. See, e.g., Exh. 94 (sampling of representative complaints).

153. These complaints came from a wide range of angry users, including teachers (Exh. 95), military commanders (Exh. 96), single parents (Exh. 97) and corporate executives (Exh. 98). Even Direct Revenue's investors and advertisers complained to the individual

respondents about being infected with the company's spyware. One partner at Insight Partners, Direct Revenue's principal venture capital investor, complained:

I understand that a couple of people I know have "caught" a really bad "adware" object (one person said "the most aggressive pop up that I have ever seen") called Aurora (tracked to Direct Revenue) that apparently has caused great problems on their computers and they have had serious problems trying to figure out how to remove it. They both said that they have no idea how they caught it. You and Blair should make sure that the company is squeaky clean in its approach and also make sure there is no liability back to their firm. . . . This looks like a pretty serious issue.

See Exh. 99 (email from D. Parekh to J. Abram dated May 18, 2005); Exh. 100 (email from J. Abram to S. Krause et al. dated May 16, 2005) (forwarding complaint from Direct Revenue's other venture capital investor, TICC).<sup>22</sup> See also Exh. 102 (email from D. Doman to A. Murray et al. dated June 17, 2005) (forwarding complaint from executive of ad network FastClick, which ceased using Direct Revenue after executive's computer was infected with Aurora without his consent).

154. In addition to receiving countless consumer complaints, each of the individual respondents doggedly tracked several anti-spyware websites that regularly exposed Direct Revenue's misleading tactics. These sites regularly gave precise descriptions of the deceptions used by Direct Revenue and its affiliates. See, e.g., Exh. 103 (email from D. Doman to J. Abram, A. Murray, D. Kaufman, R. Hook et al. dated December 16, 2004) (discussing posting on the popular site SlashDot.com, exposing Direct Revenue's distribution and retention tactics);

---

<sup>22</sup> Insight Partners itself received complaints from angry consumers about Direct Revenue's spyware programs. Insight responded by asking Direct Revenue to remove reference to Insight from the Direct Revenue website. See Exh. 101 (email from D. Parekh to J. Abram dated June 25, 2005).

Exh. 104 (email from M. Stanghed to A. Murray dated July 8, 2004) (tracking anti-spyware activist Ben Edelman); Exh. 109 (tracking criticism of Pest Patrol website); Exh. 105 (email from C. Dowhan to J. Abram, A. Murray, D. Kaufman, R. Hook dated April 5, 2004) (tracking website created specifically to criticize Direct Revenue practices).

155. As the company and its base of infected users grew, mainstream publications also began to criticize the company for deceptive spyware downloads and reinstalls after deletion. In December 2004, Newsweek published an expose about the company, harshly criticizing its business practices. See, e.g., Exh. 106. Yet the individual respondents eventually became biased even about the shame of operating one of the most reviled companies in America. Forwarding a critical Information Week article, one of the company's venture capital partners cavalierly noted, "At least we're not Ebola." See Exh. 107 (email from D. Parekh to J. Abram, A. Murray, D. Kaufman dated March 31, 2005).<sup>23</sup>

156. The individual respondents also knew that most internet security firms listed Direct Revenue's spyware as one of the most dangerous threats on the internet. See, e.g., Exh. 109 (email from R. Hook to J. Abram, A. Murray, D. Kaufman et al. dated August 5, 2004) (noting that Yahoo! Anti-Spy program identified Direct Revenue's VX2 program as #2 new pest on the internet).<sup>24</sup> Rather than remedy their company's distribution practices, the individual respondents instead conducted tests to see what percentage of infected machines had Yahoo!'s

---

<sup>23</sup> Ebola is a highly contagious, usually fatal disease that causes high fever, vomiting and massive internal bleeding in its victims. See Exh. 108 (Wikipedia entry for Ebola).

<sup>24</sup> Yahoo!'s identification of Direct Revenue as a primary spyware threat is particularly telling (if hypocritical) in that Yahoo! itself profited by providing Direct Revenue with search results for its 404 redirect programs. See supra fn. 18.

anti-spyware tool running, and whether Direct Revenue successfully reinstalled after removal by Yahoo!. See id. (confirming that Direct Revenue’s spyware reinstalled after deletion).

157. So well tuned were Abram, Murray and Kaufman to complaints and criticisms about their company’s deceptive practices that they received daily automated search updates from Google.com for the terms “Direct Revenue,” “ABetterInternet” and “MyPCTuneUp,” in order to keep abreast of ongoing criticism. See, e.g., Exh. 110 (email from R. Ross to A. Murray et al. dated April 29, 2005). Eight of ten results on the first page of a representative Google search for DirectRevenue lead to websites that pinpoint and severely criticize many of the same misleading practices alleged in this Affirmation. See Ip Aff. ¶¶ 266-270.

158. While the individual respondents obsessively monitored the many websites and blogs that criticized their company, they rarely revised Direct Revenue’s practices based on the criticisms. Instead, they threatened lawsuits against such websites and such organizations, without regard to validity or merit. See, e.g., Exh. 111 (email from J. Abram to A. Schwartz dated May 14, 2005) (threatening critic from prominent non-profit Center for Democracy and Technology that “we’ll need to speak to you immediately to avert immediate legal action against you and the CDT”); Exh. 112 (email from S. Edelman to J. Abram dated May 11, 2005) (email from legal counsel indicating success in coercing removal of post critical of Direct Revenue from anti-spyware blog). In at least one instance, the respondents even hired a private investigator to threaten a critic who refused to bow to Direct Revenue pressure. See Exh. 113 (email from G. Kibel to J. Abram et al. dated May 31, 2005) (adding, “perhaps a letter to his true home address showing that we know more about him will have results”).

The Individual Respondents Accepted the Benefits  
Of Their Distributors' Deceptive and Illegal Actions

159. Even though they knew that consumers had not consented to install their spyware, the individual respondents decided not only to show ads to illegally obtained users, but also to remotely update their spyware (and install more spyware) on those users' computers. The individual respondents ignored the suggestion of their own Chief Technology Officer that they use their "updater" software to remotely uninstall spyware programs that they believed had been deceptively installed. See, e.g., Exh. 82 (email from D. Doman to J. Abram, A. Murray, D. Kaufman et al. dated May 5, 2005) (suggesting that the company remotely uninstall improperly install spyware). Instead, the individual respondents continued to accept the stream of illicit profits.<sup>25</sup>

160. The individual respondents even authorized the repeated reinstallation of deceptively installed spyware if a user tried to remove the programs through any means other than MyPCTuneUp.com. As Direct Revenue's vice-president for distribution aptly summed up the company's philosophy:

The user's confusion about why [Direct Revenue spyware is] coming down to the machine later should not stop us from installing. It's arguable that they don't know what they're getting no matter when we get installed."

See Exh. 114 (email from C. Dowhan to J. Abram, A. Murray, D. Kaufman dated March 8, 2005).

---

<sup>25</sup> After Direct Revenue became aware of the OAG's investigation, it remotely uninstalled spyware programs that had been distributed by two of its distributors – ICMD and IMGiant. See Exh. 6 (letter from N. Klausner to K. Dreifach et al. dated January 17, 2006). Nevertheless, those installs represent a small fraction of the spyware programs that the respondents knew or should have known were distributed through deceptive means.

2. The Individual Respondents Directed That Direct Revenue's Programs Be Made Extremely Difficult to Identify and Remove

161. The individual respondents also directed that Direct Revenue's spyware programs were to be unusually difficult to identify and remove. See supra ¶¶ 116-128. All, for example, were involved in Direct Revenue's decision to prevent the vast majority of its spyware programs from appearing in a user's Add/Remove directory. See, e.g. Ip Aff. ¶¶ 21, 162, 219, 247, 257; Thomas Aff. ¶¶ 20, 35, 82; see also Exh. 115 (email from D. Doman to J. Abram, A. Murray, D. Kaufman, R. Hook et al. dated May 2, 2005) (recognizing that Direct Revenue's spyware was listed in Add/Remove for one or two small distributors, at those distributors' requests).

162. The individual respondents consciously selected the confusing MyPCTuneUp method for **uninstall** over more user-friendly, transparent options. In fact, more than a year earlier, Direct Revenue had experimented with offering an "Add/Remove" option to users infected with their spyware – thus giving users an effective means of eliminating the spyware. But the individual respondents quickly removed the entry when it led to an "incredibly scary" number of uninstalls by consumers asserting autonomy over their desktops. See Exh. 116 (email from J. Abram to A. Murray, D. Kaufman, R. Hook et al. dated February 16, 2004) (announcing intention to "take[] us out of add/remove" as a means of "fighting churn").

163. The individual respondents even directed Direct Revenue to access users' computers (without consent) to "update" already installed spyware programs to remove any Add/Remove entries. See Exh. 117 (email from J. Abram to A. Murray, D. Kaufman, R. Hook dated March 3, 2004); Exh. 118 (email from R. Hook to J. Abram, A. Murray, D. Kaufman et al. dated March 5, 2004). Days later, the individual respondents celebrated this decision to

surreptitiously remove the “Add/Remove” option for its spyware programs:

If Add/Remove entries were really increasing our user opt-out rates (and I think they were) this [decision to remove the “Add/Remove” option] should cause our rate of growth to increase pretty significantly. Like dropping sandbags off a hot air balloon.

See Exh. 119 (email from R. Hook to A. Murray et al. dated March 9, 2004).

164. Direct Revenue’s distributor Morpheus (unlike most) insisted upon providing users with an option in Add/Remove. See Exh. 115. Even then, the individual respondents were reluctant to allow users this option, even for such a minor distributor. Kaufman, for example, argued for “less user friendly uninstall methodologies”:

[M]y thinking had been that the Morpheus client would be a “test case.” If the uninstall rates weren’t too high, then great – we’d learn that putting an easy uninstall on other distribution would be ok to do. But if the uninstall rates were unacceptably high, then we’d have learned that we need to experiment with other uninstall methodologies to lower the uninstall rates to an “acceptable” level. If the data Rod is quoting is accurate, I personally consider the Morpheus uninstall rate to be unacceptably high. If we agree to this, then we need to experiment with less user friendly uninstall methodologies.

See Exh. 52 (email from D. Kaufman to J. Abram, A. Murray, R. Hook et al., dated February 2, 2005).<sup>26</sup>

165. Sometimes, Direct Revenue’s executives found it easiest to lie to distributors

---

<sup>26</sup> In fact, the individual respondents did resort to further deceptive practices to reduce the number of uninstalls from its Morpheus distributions: they tweaked the spyware bundled with Morpheus so that it would not display ads until 24 hours after installation. See Exh. 120 (email from C. Dowhan to J. Abram dated March 1, 2005). As Vice-President of Distribution Chris Dowhan explained, “If we add a 1 day delay, we might reduce the correlation between the Morpheus download and why they are seeing ads — hopefully creating less of a path to what they should uninstall.” See id. Both Abram and Hook each remarked that this was a “good idea.” See id.

about their lack of an Add/Remove option. For example, Direct Revenue explicitly promised its distribution partner IST that Direct Revenue's spyware would be listed in Add/Remove, but later secretly deleted the Add/Remove entry. See Exh. 121 (email from C. Dowhan to J. Abram et al. dated September 29, 2004) ("But to be specific on this one, we promised them [IST] an uninstall and then when we thought they weren't watching anymore, removed it on purpose. This is actually a successfully managed process as opposed to something that fell between the cracks.").

166. The individual respondents knew that most users would not locate or use the unusually complex uninstall process hosted at MyPCTuneUp.com. See Exh. 52 (email from D. Kaufman to J. Abram, A. Murray, R. Hook et al. dated February 2, 2005) ("my own personal vote would be that we have NO uninstall (other than the user somehow finding his way to mypctuneup)"). They also knew that even if infected users did "somehow find" the MyPCTuneUp site, they would be highly unlikely to trust Direct Revenue to download yet more software from the company. As one user wrote Direct Revenue, "It has occurred to me that [the MyPCTuneUp website] would be an ingenious new way of inserting a virus into my computer." See Exh. 122 (email from D. Doman to J. Abram et al. dated September 8, 2004). Direct Revenue's Chief Technology Officer Doman confirmed to Abram and Murray that the customer's wariness in this regard was "quite sensible." See id.

167. The individual respondents also knew that the MyPCTuneUp utility often did not successfully remove the company's sophisticated spyware programs as promised. See, e.g., Exh. (email from D. Doman to A. Murray et al. dated September 12, 2004) (forwarding user complaint about MyPCTuneUp's failure to uninstall Direct Revenue spyware). Likewise, they knew that this convoluted uninstall mechanism did not work on computers with common firewall security

programs or anti-virus programs. See Exh. 124 (email from D. Doman to J. Abram et al. dated June 8, 2005) (“The Symantec firewall issue is pretty serious in that it blocks our uninstall from properly working and without using our uninstall the user cannot effectively remove our software without it.”); Exh. 125 (email from anonymous complainant to J. Abram et al. dated May 21, 2005) (complaint expressing refusal to “turn off my firewall to remove your [expletive] software”).<sup>27</sup>

168. By early 2005, faced with a decision whether to correct such uninstall problems, the individual respondents opted to leave the obstacles in place. Plainly aware of these persistent user difficulties, Hook nonetheless recommended to the other respondents, “Based on the [relatively high] uninstall numbers we saw from [M]orpheus yesterday, I think we need to continue to distribute a healthy chunk of unbranded clients,” i.e., ad campaigns that, unlike Morpheus, hid the Direct Revenue brand name and thus confused consumers who might otherwise discover how to uninstall. See Exh. 128 (email from R. Hook to C. Dowhan et al. dated February 3, 2005); see also Exh. 129 (email from R. Hook to J. Abram et al. dated April 19, 2005) (instructing that Aurora program not be placed in Add/Remove: “Don’t put it in add/remove. . . . Morpheus is in add/remove and we know the optout rates are huge.”).

169. Finally, months later, Direct Revenue added to its spyware consistent branding and an Add/Remove option. See Exh. 71 (email from D. Doman to J. Abram, A. Murray, D.

---

<sup>27</sup> Respondent Abram even instructed subordinates to lie about how difficult its spyware was to uninstall. Although Direct Revenue had in fact received countless complaints from consumers about the ineffectiveness of the MyPCTuneUp utility, see, e.g., Exh. 126 (sampling of MyPCTuneUp complaints), Abram told a subordinate to falsely assure a concerned advertiser, “We have yet to hear from a customer who has failed to remove our software using our tools.” See Exh. 127 (email from J. Abram to G. Walter et al. dated June 9, 2005).

Kaufman, R. Hook et al. dated May 27, 2005) (noting that half of Direct Revenue spyware programs were “branded,” and that half of those had an entry in Add/Remove). But even then, Direct Revenue designed its spyware’s Add/Remove entry to be unusually complex and difficult to use: instead of removing the spyware simply by clicking the Add/Remove listing (as is customary), users who clicked on the listing were instructed to “go to MyPCTuneUp.” Once again (see supra ¶¶ 113, 138, 145-146, 159, 166-167) Chief Technology Officer Doman’s plea for a more transparent, user-friendly approach was rejected. See Exh. 130 (email from D. Doman to J. Abram dated May 18, 2005) (“if we choose to use the ‘more transparent’ add/remove that doesn’t just say ‘click here to go to mypctuneup and uninstall’ we can have that ready on 20 minutes notice. I know I am beating a dead horse on that – LOL”).

170. The individual respondents also knew that the company’s spyware reinstalled itself if a consumer used any other method to try to remove Direct Revenue’s spyware. See, e.g., Exh. 56 (email from D. Doman to J. Abram, A. Murray et al. dated August 31, 2004) (discussing use of “recovery mechanism[s]” named “poller” and “stubby” to reinstall spyware after deletion). For instance, Hook reported to the other individual respondents that Direct Revenue was able to reinstall its spyware after deletion by Yahoo!’s Anti-Spy program: “It found mxtarget and removed it and recommended I reboot. It left all the mxtarget registry entries and just basically disabled the BHO. It did not find the poller so we came back when I rebooted.” See, e.g., Exh. 109 (email from R. Hook to J. Abram, A. Murray, D. Kaufman et al. dated August 5, 2004) (adding, “if every user experience went like mine, we won’t even miss a beat . . .”).

3. **The Individual Respondents Participated in and Had Knowledge of the Decision to Show Misleading Ads and Install Other Spyware Programs**

171. Each individual respondent was aware of the incredibly invasive nature of Direct Revenue's spyware programs, including the vast number of pop-up ads shown to users. See, e.g., Exh. 131 (email from R. Hook to J. Abram, A. Murray, D. Kaufman et al. dated June 7, 2005) (Kaufman and Hook dismissing internal complaints that Direct Revenue was "abusing the hell out of our users").

172. Each also knew that the company's spyware showed misleading anti-spyware ads, such as the one authored by Software Online, discussed supra, ¶¶ 111-115. See, e.g., Exh. 38 (email from J. Engroff to J. Abram, A. Murray, D. Kaufman, R. Hook et al. dated January 17, 2005). In fact, on March 9, 2005, a special meeting of the individual respondents was called to discuss these misleading ads. See Exh. 132 (email from A. Pancer to D. Kaufman et al. dated March 9, 2005) (also noting weekly revenue of nearly \$90,000 from four misleading campaigns). Nevertheless, nearly two months after this discussion, Software Online's anti-spyware ad was still Direct Revenue's most profitable campaign. See Exh. 39 (email from J. Engroff to A. Murray et al. dated April 27, 2005). In fact, the company continued to run similar "purposefully confusing" ads even despite complaints from Direct Revenue's distributors. See Exh. 41 (email from D. Kaufman to J. Abram, A. Murray, R. Hook et al. dated August 16, 2005) (also remarking that "part of the trouble is that they [the distributor] have been living with our ad client for a while and feeling first-hand the user experience – both number of ads and 'quality' of our ads").

173. Finally, the individual respondents approved of Direct Revenue's use of its backdoor "updater" program to silently add yet more sophisticated versions and other spyware to

users' computers, see supra ¶¶ 129-134. See, e.g., Exh. 60 (discussing "daily maintenance" remote updates); Exh. 133 (email from R. Khan to J. Abram, A. Murray, D. Kaufman, R. Hook et al. dated May 17, 2005) (discussing remotely adding 404 redirect program to all computers with Aurora spyware program: "Hopefully, the 404 penetration will go back to 80%-90% of the US active user base."). All were also aware that Direct Revenue silently added "torpedo" programs and changed a user's security settings to remove competing spyware programs. See, e.g., Exh. 65 (email from D. Doman to J. Abram, A. Murray, D. Kaufman, R. Hook et al. dated December 21, 2004).

**G. Pre-litigation Notice**

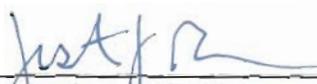
174. Pre-litigation notice as provided for in New York General Business Law § 349 and § 350-c has been given by certified mail delivered on five or more days notice to respondents. See Exh. 134 (certified letters to respondents' counsel containing Notice of Proposed Litigation).

175. Respondents repeatedly and persistently have engaged in fraudulent, deceptive and illegal acts in the distribution and installation of its spyware programs. They are responsible for saddling millions of unsuspecting consumers, including children, with untold amounts of spyware. Such practices not only harass, annoy and intrude upon users, they damage the very integrity of the internet and e-commerce: such harassment and confusion repels consumers from even using their computers.

176. Accordingly, Petitioners respectfully request that the court grant the relief requested in the accompanying Verified Petition, enjoining respondents' deceptive business practices; requiring respondents to issue an accounting; requiring respondents to disgorge any unjust enrichment derived from their illegal activities; and awarding costs and penalties as authorized by statute, and such other relief as requested herein.

WHEREFORE, the Attorney General respectfully requests that the Court grant the relief sought in the accompanying Verified Petition.

Dated April 3, 2006  
New York, New York

  
Justin Brookman