

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

NOTICE OF
VERIFIED PETITION

Index No. 401325/06

NEW YORK
COUNTY CLERK'S OFFICE

APR - 4 2006

NOT COMPARED
WITH COPY FILED

PLEASE TAKE NOTICE, that upon the annexed Verified Petition, verified on April 3 2006, and the accompanying affirmation of Assistant Attorney General Justin Brookman executed April 3, 2006, with exhibits annexed, Petitioners will move this Court at Room 130 of 60 Centre Street, New York, New York, on the 1st day of May 2006, at 9:30 o'clock in the forenoon or as soon thereafter as counsel may be heard for a Judgment and Order:

*the motion support
office
court room*

WHEREFORE, Petitioners request that this court grant relief pursuant to Executive Law § 63(12), General Business Law §§ 349 and 350, and New York common law, against Respondents by issuing an Order and Judgment as follows:

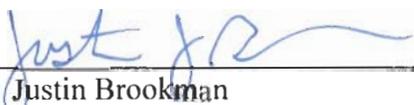
- i. permanently enjoining respondents from installing any program onto any consumer's computer, without first obtaining verifiable, affirmative consent, by which the consumer has been presented with, and knowingly consented to, receive such program;
- ii. permanently enjoining respondents from any advertising practices that contain misrepresentations or omissions regarding the software that

- consumers are to receive or download;
- iii. permanently enjoining respondents from installing any advertising, ad-serving, redirecting, or behavior monitoring program onto any consumer's computer;
 - iv. directing respondents to provide Petitioners with all records of all respondents' advertising, ad-serving, redirecting and behavior monitoring programs installed onto consumers' computers, including all records concerning or reflecting any disclosure provided to consumers prior to or during download;
 - v. directing respondents to provide Petitioners with an accounting of all revenues generated from the distribution of advertising, ad-serving, redirecting and behavior monitoring applications and that a money judgment be entered against Respondents in the sum of unjust enrichment;
 - vi. directing that a money judgment in civil penalties pursuant to G.B.L. § 350-d be entered against Respondents in favor of the State of New York based upon the sum of \$500 per each instance of a deceptive or unlawful practice;
 - vii. directing that a money judgment be entered against Respondents in favor of Petitioners in the sum of \$2000 against each Respondent, pursuant to CPLR § 8303(a)(6);

viii. granting Petitioners such other and further relief as this Court finds just and proper.

DATE: April 3, 2006
New York, New York

**ELIOT SPITZER
ATTORNEY GENERAL
OF THE STATE OF NEW YORK**


By: Justin Brookman
Internet Bureau
Attorney for Petitioner
120 Broadway, 3rd Floor
New York, New York 10271
(212) 416-8433

Of Counsel:
Kenneth M. Dreifach
Assistant Attorney General In Charge
Internet Bureau

**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,**

VERIFIED PETITION

Petitioners,

Index No. _____

-against-

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

Respondents.

-----x
The People of the State of New York, by Eliot Spitzer, Attorney General of the State of New York, allege upon information and belief that:

Preliminary Statement

1. Petitioners bring this summary proceeding (a) to permanently enjoin respondents from installing any advertising, ad-serving, redirecting or behavior monitoring program onto any user's computer; (b) to require respondents to issue an accounting of their installation of advertising, ad-serving, redirecting and behavior monitoring programs, and any monies or other consideration collected or realized from installing those programs; and (c) to require respondents to pay disgorgement of unjust enrichment, as appropriate, and penalties and costs to the State of New York.

2. Since 2002, Direct Revenue has installed more than 150 million ad-serving programs (also known as "spyware" or "adware"), directly from its own servers onto consumers' computers. During most of this period, it has rarely obtained consumers' consent to perform these installations, or given consumers anything approaching reasonable or conspicuous notice

that the spyware was being installed. Through these downloaded programs, Direct Revenue has then deluged consumers with streams of pop-up ads, for which its own advertisers have paid it millions of dollars.

3. This office has conducted an extensive investigation into the manner by which Direct Revenue places its ad-serving software onto users' computers. This investigation documented numerous deceptive methods by which Direct Revenue gained access to consumers' computers, downloaded its spyware, and even continued to access these computers over time to download further spyware. Compounding this, respondents deliberately designed their spyware to be extremely difficult for consumers to detect and remove from their computers.

4. The named individuals ("individual respondents"), Direct Revenue's founders, officers and principal owners, knew of and participated in the deceptive practices described herein. They are therefore individually liable for penalties, costs, and disgorgement, and subject to **injunctive** relief.

Parties

5. 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.

6. Petitioners bring this summary proceeding pursuant to the Attorney General's authority under Executive Law § 63(12) and General Business Law ("GBL") §§ 349-350, and his common law authority, to enjoin respondents from engaging in (1) persistent deceptive, fraudulent and illegal practices and false advertising in the distribution of spyware; (2) persistent violation of Penal Law § 156.20 (computer tampering in the fourth degree); (3) persistent

violation of New York common law prohibiting trespass to chattels; and (4) negligent hiring, supervision and retention of distributors and subdistributors.

7. Respondent DirectRevenue, LLC (“Direct Revenue”) is (and was during all relevant times) a Delaware corporation with its principal offices in New York, New York. Since 2002, **Direct Revenue** has distributed millions of spyware programs to consumers all over the world. **At all** relevant times, its founders, principal officers, and principal owners have been the four individual respondents: Joshua Abram, Alan Murray, Daniel Kaufman and Rodney Hook. **During** the relevant time period, these individuals were also the principal owners of the company. Specifically, they held 100 percent of the company’s stock shares until selling a portion of their holdings in 2004; they currently hold approximately 55 percent of the company’s stock.

8. Respondent Joshua Abram is Direct Revenue’s Executive Vice-President for Business Development. 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 New York in November 2002. Since that time, Abram has been aware of and has participated in Direct Revenue’s deceptive spyware practices. Abram is a resident of New York.

9. Respondent Alan Murray is Direct Revenue’s Chief Product Officer. Until August 2005, he served as the company’s Chief Operations Officer. Murray was one of the original four founders of Direct Revenue in November 2002. Since that time, he has been aware of and has participated in Direct Revenue’s deceptive spyware practices. Murray is a resident of New York.

10. Respondent Daniel Kaufman is Direct Revenue’s Executive Vice President for

Corporate Development. Kaufman was one of the original four founders of Direct Revenue in November 2002. Since that time, he has been aware of and has participated in Direct Revenue's deceptive spyware practices. Kaufman is a resident of New York.

11. Respondent Rodney Hook is Direct Revenue's Chief Technology Officer. Prior to August 2005, Hook's position with the company was Chief Scientist. Hook was one of the original four founders of Direct Revenue in November 2002. Since that time, he has been aware of and has participated in Direct Revenue's deceptive business practices. Hook is a resident of New York.

Statutory Framework

12. GBL § 349 empowers the Attorney General to seek injunctive relief when any person or entity has engaged in deceptive acts or practices in the conduct of any business. GBL § 350-d empowers the Attorney General to seek, inter alia, civil penalties in the amount of \$500 for each violation of GBL § 350, the False Advertising Statute, and GBL § 349, the Deceptive Practices Statute. In addition, Executive Law §§ 63(1) and 63(15) broadly empower the Attorney General to seek injunctive and equitable relief when any person or business entity has engaged in or otherwise demonstrated repeated fraudulent or illegal acts in the transaction of business. Finally, Civil Procedures Law and Rules ("CPLR") § 8303 authorizes the Court to award the Attorney General's office \$2000 in costs per respondent.

13. New York Penal Law § 156.20 provides that a person has committed computer tampering when he "uses or causes to be used a computer or computer service and having no right to do so he intentionally alters in any manner or destroys computer data or a computer program of another person."

14. Pre-litigation notice in accordance with GBL §§ 349 and 350-c has been given by certified mail delivered on five or more days notice to respondents. See accompanying Affirmation of Justin Brookman (“Brookman Aff.”) ¶ 174.

**Direct Revenue’s Repeated and Persistent
Pattern of Non-Consensual Spyware Installations**

15. The Office of the Attorney General (“OAG”) conducted an extensive investigation into the manner by which Direct Revenue places its ad-serving software onto users’ computers. This investigation documented numerous deceptive methods by which Direct Revenue gained access to consumers’ computers, downloaded its spyware, and even continued to access these computers over time to download further spyware.

16. In most cases, these spyware installations were instigated when Direct Revenue (or one of its distributors or sub-distributors) advertised to consumers “free” programs, such as screensavers or games. Once the consumers agreed to download these “free” applications, a small string of code was placed onto the consumers’ computers, which in turn instructed Direct Revenue’s servers to silently install its spyware onto the users’ desktops.

17. In this manner, known as “bundling,” Direct Revenue has installed its invasive spyware onto consumers’ computer more than 150 million times. Once on users’ desktops, Direct Revenue’s spyware programs, named, inter alia, “VX2,” “Aurora,” and “OfferOptimizer,” track consumers’ web behavior and deliver pop-up ads to them.

18. As a general rule, at no time during this process were consumers given reasonable or conspicuous notice that Direct Revenue would download its spyware – neither by Direct Revenue, nor its distributors. At best, notice of the spyware was hidden deep within a linked

“agreement” – yet deceptively omitted from the description of the “free” software that consumers understood they were downloading.

19. Compounding this invasive fraud, Direct Revenue designed its spyware so that, once downloaded, it was extremely difficult for users to detect and remove. In many instances, the spyware even reinstalled itself after removal.

20. Direct Revenue made millions of dollars in revenue, from advertisers whose pop-up ads it showed through its spyware programs. As described herein, it committed other, further deceptions and trespasses in order to capitalize on this illegal behavior, such as continuing impermissibly to access users’ computers over time to download further spyware.

21. Between November 2004 and September 2005, the OAG conducted 29 tests of web sites that distributed Direct Revenue’s spyware. In virtually every one of these tests, Direct Revenue failed to provide reasonable or conspicuous notice regarding the spyware it was about to download. These tests are described in greater detail, with relevant screen shots, in the accompanying Brookman Affirmation and Affidavits of Vanessa Ip, Joseph Rivela and Siblu Thomas.

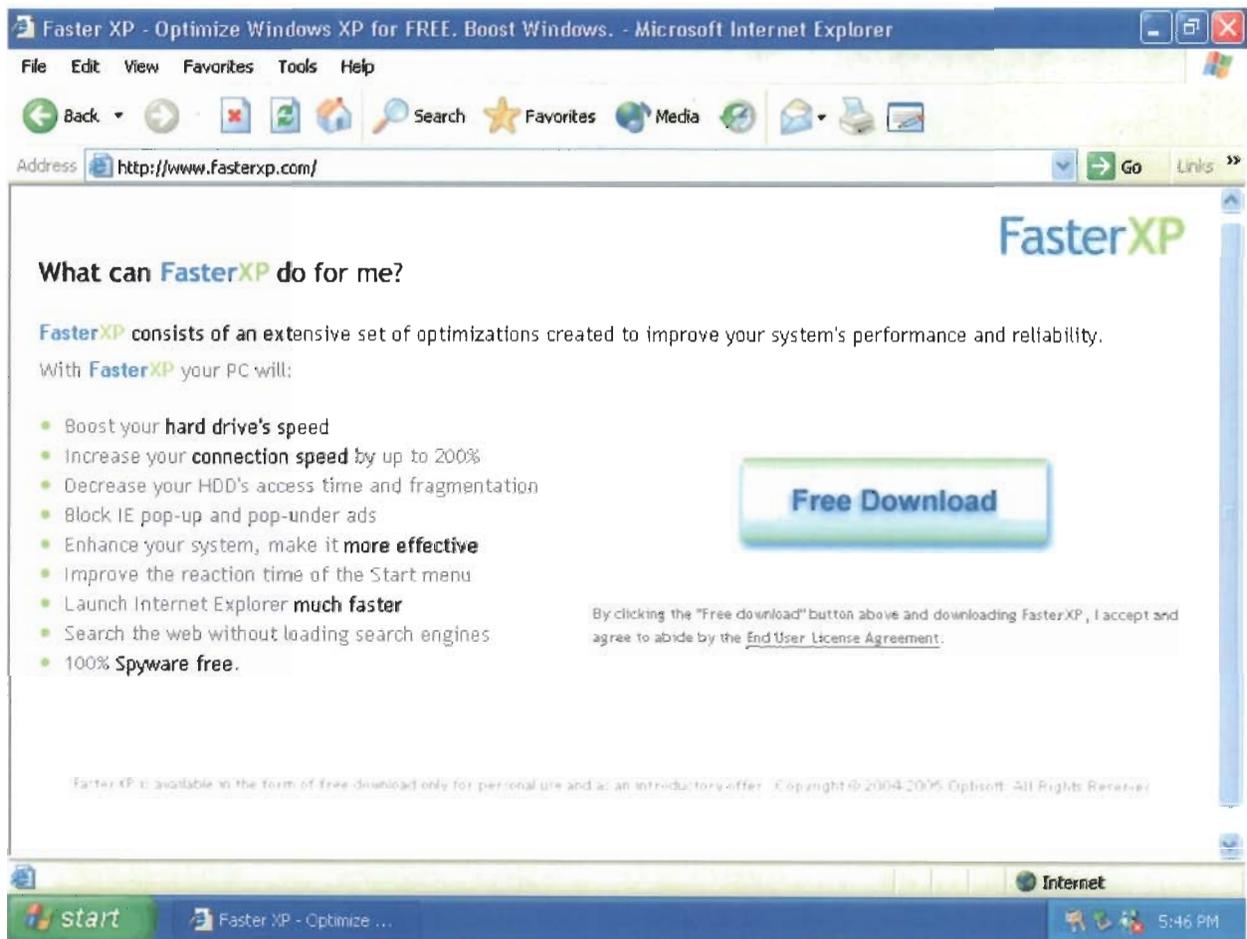
A. Deceptive Spyware Installations Disguised as “Free Software”

22. One website (of the many) that Direct Revenue has used to help it gain users and spread its spyware is FasterXP.com. This site promises “free” software to improve computer performance and increase connection speeds. See Brookman Aff. ¶¶ 35-36.

23. Yet after downloading and installing the **FasterXP** program, an OAG investigator confirmed that in addition to this “free” FasterXP software, Direct Revenue’s “Aurora” spyware had been installed onto the investigator’s test computer. See Brookman Aff. ¶ 40.

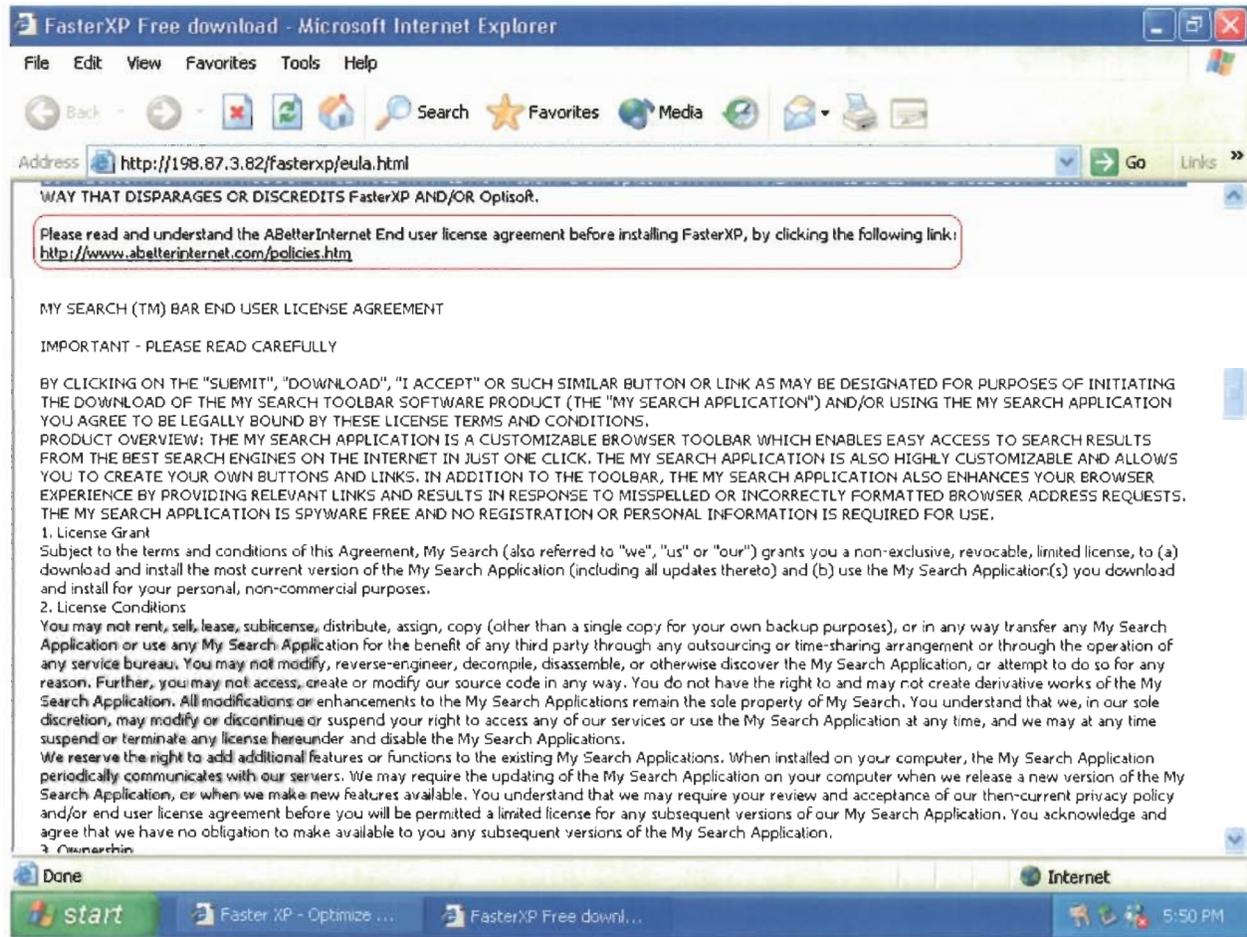
24. Direct Revenue installed its “Aurora” spyware program without reasonable or conspicuous warning or disclosure. None of the six screens the investigator had viewed on the FasterXP site – nor any of the fifteen screens shown during installation – offered any mention or hint that Direct Revenue’s spyware would be bundled with the “FasterXP” software. To the contrary, the web site falsely promised that FasterXP was “100% Spyware free.” See Brookman Aff. ¶¶ 36-39; Screen Shot No. 1, below.

SCREEN SHOT NO. 1



25. Respondents, however, purport to have obtained user consent as follows. The FasterXP.com home page contained a link (in small print) stating: “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. This license agreement was not directly presented to users, and was only available through a link. The fourth page of the eleven page “agreement,” in turn, contained the vague directive: “Please read and understand the ABetterInternet End user license agreement before Installing FasterXP.” See Screen Shot No. 2, below. This second link led to yet another, lengthy license agreement which finally disclosed that “ABetterInternet” (a subsidiary of Direct Revenue) would install advertising software on the user’s computer. See Brookman Aff. ¶¶ 36, 39.

SCREEN SHOT NO. 2 (reference to ABetterInternet license agreement circled)



26. Clearly, no ordinary consumer would wade through two separate license agreements expecting to find notice of a hidden, bundled spyware program. By failing to give valid notice, or get user consent, prior to downloading its spyware, **Direct Revenue** has profited greatly: it has downloaded millions of ad-serving spyware programs, which it has monetized through ad sales.

27. The OAG's investigators recorded similar practices at several other websites, each of which offered "free" programs without conspicuously disclosing the **Direct Revenue** spyware

programs with which they were bundled. In each case, disclosure of spyware programs was contained either within a lengthy, linked license agreement, or, in some cases, there was no disclosure at all. These deceptive practices were recorded on sites operated by Direct Revenue, as well as sites operated by Direct Revenue's contracted distributors. See Brookman Aff. ¶¶ 42-59.

B. Deceptive "ActiveX" Spyware Installations

28. Direct Revenue also has distributed its spyware through deceptive "ActiveX" advertisements, through which it offers users allegedly "free" software.¹ See Brookman Aff. ¶¶ 60-63. When doing so, Direct Revenue has not given consumers reasonable or conspicuous notice that this "free" software (such as a screensaver or game) comes bundled with Direct Revenue's spyware.

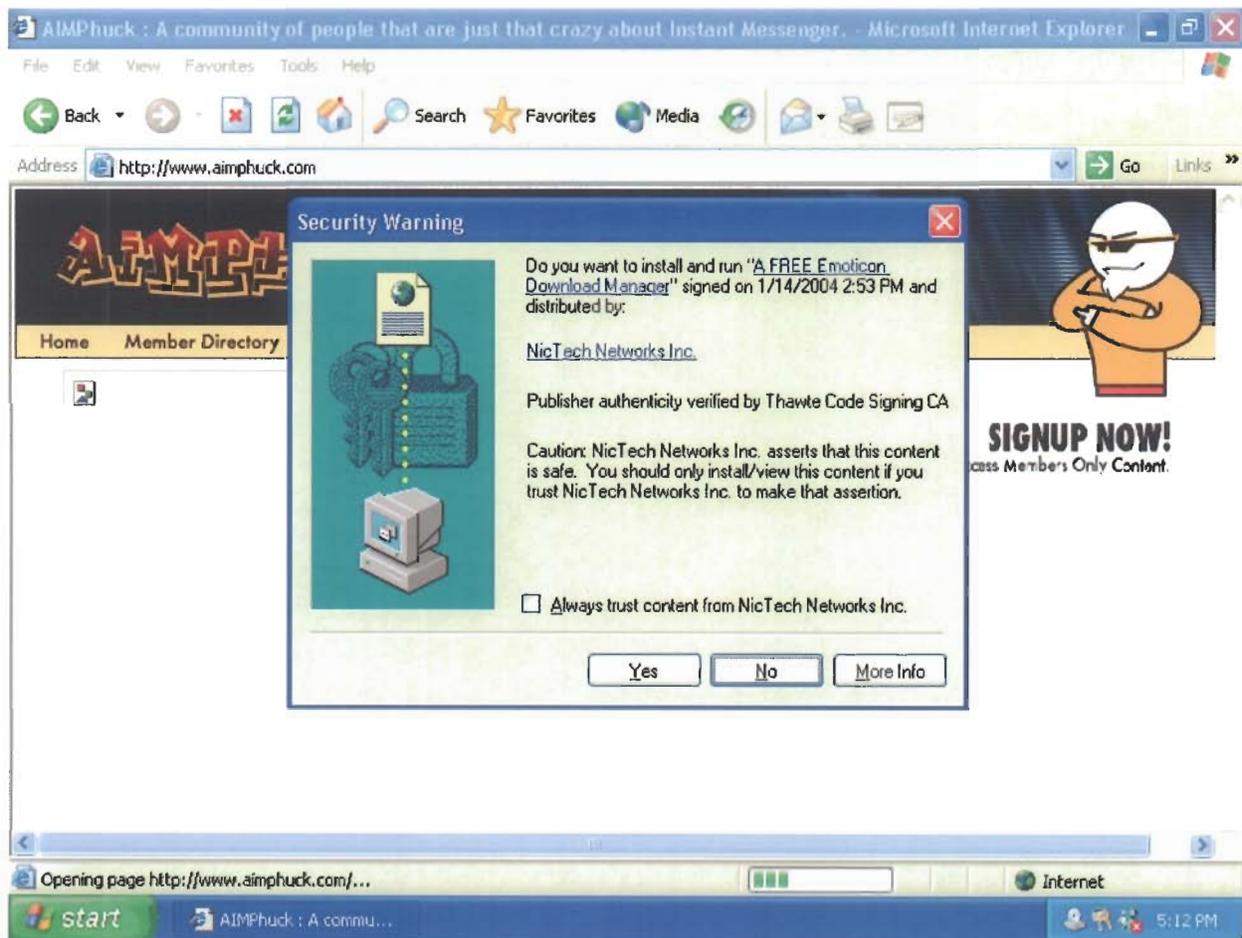
29. In some cases, these deceptive ActiveX advertisements have been designed by Direct Revenue itself, and in other cases they have been designed by Direct Revenue's distributors or subdistributors. In either case, when consumers agree to receive the advertised "free" program, Direct Revenue itself directly installs its undisclosed spyware in addition to that program.

30. Direct Revenue and its distributors have placed their ActiveX advertisements on a wide range of websites, including fan sites for popular entertainers and websites that provide popular song lyrics.

¹ ActiveX is a Microsoft technology that allows web content providers to run interactive programs on users' computers, usually by providing users with a modal box in the form of a "security warning," requiring a user to consent to download, or reject, a given program. See Brookman Aff. ¶¶ 60-62.

31. For instance, when an OAG investigator visited AIMPhuck.com, a site offering images and add-ons for instant messaging programs, an ActiveX “Security Warning” popped up asking whether to install “a FREE Emoticon Download Manager.”² See Screen Shot No. 3, below. Although the investigator repeatedly declined the installation offer, prompts continued to pop-up, each requesting installation. None of these prompts disclosed Direct Revenue’s spyware programs. See Brookman Aff. ¶¶ 72-73.

SCREEN SHOT NO. 3



² “Emoticons” are small animations, such as a smiley face, that instant messaging users often include in their online conversations.

32. After finally consenting to the installation of “FREE Emoticon Download Manager,” the OAG investigator determined that Direct Revenue’s spyware had also been installed on the test computer. At no point had the investigator received any notice of or disclosure about Direct Revenue’s spyware programs. See Brookman Aff. ¶¶ 72-74.

33. Investigators documented several other sites hosting similar deceptive “ActiveX” advertisements that distributed Direct Revenue spyware. See Brookman Aff. ¶¶ 64-71, 75-89. These “advertisements” were distributed both by Direct Revenue directly, and by its third party distributors. As always, notice of Direct Revenue’s spyware either was provided merely in a linked license agreement, or not at all.

C. Spyware Installations Through Security Vulnerabilities

34. The OAG’s investigators also documented instances in which Direct Revenue’s spyware was installed through malicious code that exploited security vulnerabilities in Microsoft’s web browser and operating system. These “drive-by” downloads evaded even any theoretical opportunity for notice to, and consent by, users. In such instances, simply visiting a given website infected a user’s computer with spyware programs. See Brookman Aff. ¶¶ 90-91.

Respondents are Factually and Legally Responsible For the Deceptive Downloads of Their Own Spyware

35. Respondents are factually and legally responsible for all such instances in which their spyware was deceptively distributed, whether with the assistance of Direct Revenue’s distributors (or subdistributors) or in instances when Direct Revenue acted alone. As detailed in the Brookman Affirmation, respondents had general and/or constructive knowledge and, in many

cases, specific knowledge, that their distributors were using deceptive means to initiate the process by which Direct Revenue installed spyware on users' desktops. See Brookman Aff. ¶¶ 94, 137-160.

36. Respondents made virtually no effort to police their distributors, or to establish any effective controls ensuring, or even promoting or encouraging, user notice and consent. See Brookman Aff. ¶¶ 95-101

37. Moreover, even in cases where Direct Revenue's spyware was bundled with third party software, Direct Revenue itself (as opposed to its distributors) directly installed its own spyware on users' desktops. Accordingly, in all such cases, Direct Revenue thus was directly responsible for the non-consensual installation of its own spyware. See Brookman Aff. ¶¶ 24, 148.

38. Although respondents knew that Direct Revenue's distributors were engaging in deceptive practices, it was only after the OAG served respondents with a subpoena in May 2005 that the company took significant steps to modify these deceptive distribution methods. See Brookman Aff. ¶¶ 98-101.

39. Direct Revenue continues to monitor and serve ads to millions of consumers who previously were deceptively infected with its spyware. See Brookman Aff. ¶ 102.

**Direct Revenue's Spyware is
Invasive, Harmful, and Very Hard to Remove**

40. Direct Revenue's spyware is extremely invasive and burdensome to consumers. It generates a persistent stream of pop-up advertisements. Even worse, it allows Direct Revenue permanent, stealth "backdoor" access to consumers' computers. Worse still, Direct Revenue has

used this backdoor to install even more sophisticated versions of its spyware onto users' desktops, and to install other spyware programs.

41. In order to avoid detection, Direct Revenue has hidden its spyware in various manners, discussed below, and has specifically designed its spyware to strenuously resist consumers' efforts to uninstall it.

A. Direct Revenue's Spyware Displays Incessant, Deceptive Pop-up Ads

42. Once installed, Direct Revenue's spyware displays a persistent stream of pop-up ads. These ads are often delivered less than a minute apart, and are so disruptive and annoying that the individual respondents themselves have described them as "hammering" or "abusing" consumers. See Brookman Aff. ¶¶ 105-108.

43. In order to select which ads to display, Direct Revenue's spyware monitors the websites users visit, as well as information they type into web forms, such as search engines (also known as "clickstream data"). See Brookman Aff. ¶ 109.

44. Many of the ads that Direct Revenue has displayed promote "security" and "anti-spyware" programs. In order to trick users into purchasing such anti-spyware software – and exploit their fear of products such as Direct Revenue's – these ads often mimic prompts from the user's own computer, e.g., sent by Microsoft's Windows operating system. In **this way**, Direct Revenue has taken advantage of consumers who were unwittingly **infected with Direct Revenue's** spyware. See Brookman Aff. ¶¶ 111-115.

B. Direct Revenue's Spyware Avoids Detection and Removal

45. Direct Revenue designs its spyware to be extremely **difficult** for consumers to detect and remove from their computers. First, as described supra, **Direct** Revenue has failed to

inform consumers that its software has been installed on their computers. See Brookman Aff. ¶¶ 21-91.

46. Further, Direct Revenue has designed its spyware in a manner that prevents it from being listed in the commonly accessed Windows “Programs” folder. Nor is the spyware listed in the commonly accessed “All Programs” list, located through the Windows “Start” button. Instead, Direct Revenue scatters its spyware files all across a user’s computer, hiding them in unlikely locations, with randomly-generated names, and even ascribing to those files false modification dates. See Brookman Aff. ¶¶ 116-117.

47. Further compounding user confusion, Direct Revenue has designed its spyware programs in a manner such that when users have uninstalled the program with which the spyware was bundled (e.g., the FasterXP program described supra), Direct Revenue’s spyware programs have remained behind, installed and fully operational. Direct Revenue has also failed to provide within any of its files or folders an “uninstall” utility, i.e., a small file that can be double-clicked to remove a program. See Brookman Aff. ¶¶ 119-120.

48. Until recently, Direct Revenue also designed its spyware in such a manner to prevent it from inclusion in Windows “Add/Remove Programs” utility. “Add/Remove” is the most common mechanism by which consumers uninstall programs from their computers. See Brookman Aff. ¶¶ 121-126.

49. Direct Revenue also has designed its spyware to resist any attempts to either manually delete the programs, or to delete them with common, anti-spyware programs. In fact, in the OAG’s own tests, Direct Revenue’s spyware reinstalled itself even after repeated attempts by investigators to delete it. See Brookman Aff. ¶¶ 127-128.

C. Once Downloaded, Direct Revenue's Spyware Surreptitiously Installs Yet More Spyware and Other Programs

50. In addition to its ad-serving, user-tracking functionality, Direct Revenue has installed onto users' computers secret "updater" programs giving the company permanent remote access to all infected computers. Direct Revenue has used this "backdoor" frequently, and at times on a daily basis, performing millions of silent "updates" each month on users' computers since the company's founding in 2002. See Brookman Aff. ¶¶ 129-130.

51. Direct Revenue profitably has used this backdoor access to install still more unwanted spyware programs onto users' computers, including other companies' spyware. For instance, it has used this access to install programs redirecting mistyped or unavailable web addresses to Direct Revenue's proprietary search engine web site. It has also used this backdoor to install additional pop-up ad programs, on behalf of other spyware companies. See Brookman Aff. ¶ 131.

52. Likewise, Direct Revenue regularly has used this backdoor to install increasingly sophisticated versions of its own pop-up programs, each designed to be less easily detected or removed than the last. See Brookman Aff. ¶¶ 133.

53. No notice has ever been given to consumers about any of these remote updates. See Brookman Aff. ¶¶ 132, 134.

Individuals Abram, Murray, Kaufman and Hook Each Knew of and Participated in the Above Unlawful Practices

54. Respondents Abram, Murray, Kaufman and Hook founded Direct Revenue in 2002. Since that time, they have overseen and directed the company's operations. Spyware has been the company's primary, if not only, line of business. See Brookman Aff. ¶¶ 135-136.

55. Numerous internal emails among the individual respondents demonstrate that each knew that Direct Revenue spyware was widely distributed to consumers absent anything approaching reasonable or conspicuous notice to and consent from users. Despite their knowledge of these circumstances, Abram, Murray, Kaufman and Hook permitted these deceptive downloads to continue, and personally profited from them. See Brookman Aff. ¶¶ 137-160.

56. The individual respondents directed that Direct Revenue's spyware be extremely difficult to detect and remove. For example, they directed that their software be designed so that users could not remove the company's spyware using "Add/Remove," only revising this practice after receiving the OAG's subpoena. The individual respondents also knew that Direct Revenue's spyware would resist removal and reinstall itself if a user attempted to delete the programs manually or with commonly-available anti-spyware programs. See Brookman Aff. ¶¶ 161-170.

57. The individual respondents also knew that the company "hammered" users with deceptive anti-spyware ads, and that the company used its backdoor "updater" programs to install ever more sophisticated versions of its spyware, and to install additional spyware. See Brookman Aff. ¶¶ 171-173.

**FIRST CAUSE OF ACTION
(DECEPTIVE ACTS AND PRACTICES)**

58. GBL § 349 makes unlawful "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any services in [New York]."

59. By repeatedly and persistently engaging in the acts and practices described above,

Respondents have repeatedly and persistently engaged in deceptive acts and practices in violation of GBL § 349.

60. Respondents' violations of GBL § 349 constitute repeated and persistent illegal conduct in violation of Executive Law § 63(12).

**SECOND CAUSE OF ACTION
(FALSE ADVERTISING)**

61. GBL § 350 makes unlawful "false advertising in the conduct of any business, trade or commerce or in the furnishing of any service in the state."

62. By repeatedly and persistently engaging in the acts and practices described above, respondents have repeatedly and persistently engaged in false advertising in violation of GBL § 350.

63. Respondents' violations of GBL § 350 constitute repeated and persistent illegal conduct in violation of Executive Law § 63(12).

**THIRD CAUSE OF ACTION
(NEGLIGENT SUPERVISION)**

64. New York common law prohibits the failure to use such care as a reasonably prudent and careful person in the hiring, supervision and retention of third-parties, including third-parties who distribute spyware programs to computer users across the internet.

65. By repeatedly and persistently engaging in the acts and practices described above, respondents have repeatedly and persistently engaged in negligent hiring, supervision and retention of distributors and subdistributors in violation of New York common law, and therefore are liable for fraudulent, illegal and deceptive practices, including violations of GBL §§ 349-350, committed by such persons.

66. These violations likewise constitute repeated and persistent illegal conduct in violation of Executive Law § 63(12).

**FOURTH CAUSE OF ACTION
(TRESPASS TO CHATTELS)**

67. New York common law prohibits the intentional intermeddling with a chattel, including a computer, in possession of another that results in the deprivation of the use of the chattel or impairment of the condition, quality or usefulness of the chattel.

68. By repeatedly and persistently engaging in the acts and practices described above, respondents have repeatedly and persistently engaged in trespass to chattels in violation of New York common law.

69. Respondents' violations of New York common law of trespass to chattels constitute repeated and persistent illegal conduct in violation of Executive Law § 63(12).

**FIFTH CAUSE OF ACTION
(COMPUTER TAMPERING IN THE FOURTH DEGREE)**

70. Penal Law § 156.20 provides that a person has committed computer tampering when he "uses or causes to be used a computer or computer service and having no right to do so he intentionally alters in any manner or destroys computer data or a computer program of another person."

71. By repeatedly and persistently engaging in the acts of practices described above, respondents have repeatedly and persistently engaged in false advertising in computer tampering in the fourth degree.

72. Respondents' violations of Penal Law § 156.20 constitute repeated and persistent illegal conduct in violation of Executive Law § 63(12).

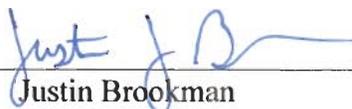
WHEREFORE, Petitioners request that this court grant relief pursuant to Executive Law § 63(12), General Business Law §§ 349 and 350, and New York common law against Respondents by issuing an Order and Judgment as follows:

- i. permanently enjoining respondents from installing any program onto any consumer's computer, without first obtaining verifiable, affirmative consent, by which the consumer has been presented with, and knowingly consented to, receive such program;
- ii. permanently enjoining respondents from any advertising practices that contain misrepresentations or omissions regarding the software that consumers are to receive or download;
- iii. permanently enjoining respondents from installing any advertising, ad-serving, redirecting, or behavior monitoring program onto any consumer's computer;
- iv. directing respondents to provide Petitioners with all records of all respondents' advertising, ad-serving, redirecting and behavior monitoring programs installed onto consumers' computers, including all records concerning or reflecting any disclosure provided to consumers prior to or during download;
- v. directing respondents to provide Petitioners with an accounting of all revenues generated from the distribution of advertising, ad-serving, redirecting and behavior monitoring applications and that a money judgment be entered against Respondents in the sum of unjust enrichment;

- vi. directing that a money judgment in civil penalties pursuant to GBL § 350-
d be entered against Respondents in favor of the State of New York based
upon the sum of \$500 per each instance of a deceptive or unlawful
practice;
- vii. directing that a money judgment be entered against Respondents in favor
of Petitioners in the sum of \$2000 against each Respondent, pursuant to
CPLR § 8303(a)(6);
- viii. granting Petitioners such other and further relief as this Court finds just
and proper.

DATE: April 3, 2006
New York, New York

**ELIOT SPITZER
ATTORNEY GENERAL
OF THE STATE OF NEW YORK**


By: Justin Brookman
Internet Bureau
Attorney for Petitioners
120 Broadway, 3rd Floor
New York, New York 10271
(212) 416-8433

Of Counsel:
Kenneth M. Dreifach
Assistant Attorney General in Charge
Internet Bureau

**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

VERIFICATION

Index No.: _____

STATE OF NEW YORK)
) **ss.:**
COUNTY OF NEW YORK)

KENNETH M. DREIFACH, being duly sworn, deposes and says:

I am the Assistant Attorney General in Charge of the Internet Bureau in the office of ELIOT SPITZER, Attorney General of the State of New York, and am duly authorized to make this verification.

I have read the foregoing petition and know the contents thereof, which is to my knowledge true, except as to matters stated to be alleged upon information and belief, and as to those matters, I believe them to be true. The grounds of my belief as to all matters stated upon information and belief are investigatory materials contained in the files of the Attorney General's office.

The reason this verification is not by petitioners is that petitioners are a body of politic and the Attorney General is their duly authorized representative.



KENNETH M. DREIFACH

Sworn to before me
this 3rd day of April 2006

KAREN A. GEDULDIG
Notary Public, State of New York
No. 02GE6087196
Qualified in New York County
Commission Expires February 10, 2007



Karen A. Geduldig
Notary Public