AFFIDAVIT OF JOSEPH RIVELA

State of New York)
) ss.:
County of New York)

I, Joseph Rivela, hereby declare as follows:

1. I am an Investigator with the Internet Bureau of the New York State Attorney General's Office, a position I have held since December 2004. My work address is 120 Broadway, Third Floor, New York, NY 10271. I make this declaration based upon my personal knowledge of the facts set forth herein.

2. Between July 2005 and August 2005, I conducted a number of investigative tests, through Attorney General's Office undercover computers, to record "spyware" or "adware" from Direct Revenue, LLC ("Direct Revenue") being uploaded and installed onto computers without notice or consent. I have set forth the results of those tests herein, including the websites from which the downloads occurred, and the disclosures – or lack thereof – presented to users. I have attached as exhibits hereto all relevant screen shots of these tests.

Wallpapers4U.com: "Browser Enhancement Installation" Download

3. On July 21, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, NY. I ran scans for existing spyware on the computer's hard drive, using the programs Ad-Aware SE Personal Edition[1] and Spybot Search &

[1] Ad-Aware is an anti-spyware program distributed by Lavasoft. According to the company's website (www.lavasoftusa.com), "Ad-Aware is designed to provide advanced protection from known Data-mining, aggressive advertising, Parasites, Scumware, selected traditional Trojans, Dialers, Malware, Browser hijackers, and tracking components." Ad-Aware has been awarded PC Magazine Editors' Choice Award by a panel of PC Magazine editors and leading industry experts.

Destroy.[2] At that time, the programs indicated the hard drive to be free of spyware. (*See Exhibit A-1, which are true and correct images of the result screens.*)

4. I opened the C:\Program Files folder to view a listing of the seventeen files located within that folder. *(See Exhibit A-2, which is a true and correct image of the window.*)

5. I next opened Internet Explorer and the <www.msn.com> start page appeared. *(See Exhibit A-3, which is a true and correct image of the browser window.)*

6. In the address bar, I typed the website address <www.wallpapers4u.com> and the "Wallpapers 4 U" homepage appeared. Upon viewing the Wallpaper 4 U homepage, a pop-up window was immediately displayed titled "Browser Enhancement Installation." The window advertised "a free browser enhancement . . . available to be installed on your system free of charge," and stated that "By installing our software, you agree to the terms and conditions stated here." However, no "terms and conditions" were listed, nor was there even a hyperlink to a web site hosting any terms and conditions. This pop-up did not make mention of any bundled spyware programs. *(See Exhibit A-4, which is a true and correct image of the browser and pop-up window.)*

7. I clicked on the button to "CLOSE THIS WINDOW" on the "Browser Enhancement Installation" pop-up. I proceeded to close all remaining browser windows by clicking on the "X" in the top right-hand corner of each browser window. I then opened Internet Explorer and immediately received a pop-up advertisement generated by Direct Revenue's Aurora Program. *(See Exhibit A-5, which are true and correct images of the pop-up window.)*

---

[2] Spybot Search & Destroy is a program designed to "detect and remove spyware of different kinds from your computer," according to its website (www.spybot.info). The software was named the best "Anti-Spyware Scanner" of 2004 by PCWorld.com.

8. I opened the C:\Program Files folder for a listing of the files located within that folder. This listing indicated that nine folders had been added during the "Browser Enhancement Installation" download process: AdDestroyer, AutoUpdate, Bullseye Network, Cas, CashBack, CasStub, NaviSearch, Save and VBouncer. Direct Revenue's Aurora program was not listed. (*See Exhibit A-6, which is a true and correct image of the window.*)

9. I closed the C:\Program Files folder and proceeded to the C:\WINDOWS directory. Ten additional files had been added to the directory since the "Browser Enhancement Installation" download, including the Direct Revenue files "AuroraHandler.dll," "Nail," and "mfqacxxndm." The listed "Date Modified" for each of the files was November 8, 2001; April 5, 2003; and October 3, 2003, respectively. *(See Exhibit A-7, which are true and correct images of the window.)*

10. I closed the C:\WINDOWS directory and launched the Add/Remove utility through the Windows Control Panel. There I was offered the option to change or remove AdDestroyer, CashBackBuddy, NaviSearch, SaveNow, The BullsEye Network, Virtual Bouncer and the Windows AFA Internet Enhancement. Although there was no listing for Aurora, there was a listing for "The ABI Network - A Division of Direct Revenue." *(See Exhibit A-8, which is a true and correct image of the window.)*

11. I closed Add/Remove and ran a scan for existing spyware on the computer's hard drive using Ad-Aware SE Personal Edition. The scan identified 615 objects, including 51 VX2[3] registry keys, files and folders. (*See Exhibit A-9, which is a true and correct images of the scan*

[3] "VX2" is the name of an early variant of Direct Revenue's software. Ad-Aware usually identifies all Direct Revenue spyware files and objects as "VX2."

results.)

12. I then ran a scan for existing spyware on the unit's hard drive using Spybot Search & Destroy. That scan identified 150 "problems," including at least 22 entries identified as AbetterInternet[4] programs. *(See Exhibit A-10, which are true and correct images of the scan results.)*

13. I logged onto the same undercover computer once again on July 26, 2005. I launched the Add/Remove utility through the Windows Control Panel and was offered the option to change or remove "The ABI Network - A Division of Direct Revenue," which was still listed among the currently installed programs. *(See Exhibit A-11, which is a true and correct image of the window.)*

14. I clicked on the button marked "Change/Remove" and I was immediately directed to an Internet Explorer browser window with the directory path C:\WINDOWS\abiuninst.htm displayed in the address bar of the browser window. This window directed me to go to the website <www.mypctuneup.com> to remove the "the ABI Network software." *(See Exhibit A-12, which is a true and correct image of the browser window.)*

15. Following the instructions provided, I copied the URL <www.mypctuneup.com> from the displayed text and then entered it into the address bar by using the "paste" function. I was then directed to the MyPCTuneUp homepage. *(See Exhibit A-13, which are true and correct images of the browser window.)*

16. I then clicked on the button marked "Uninstall" located on the left side of the

---

[4] A Better Internet (BetterInternet, LLC) is a division of Direct Revenue. Spybot search and Destroy often identifies Direct Revenue spyware files and folders as "AbetterInternet."

browser window and was directed to <www.mypctuneup.com/evaluate.php>, a web page providing instructions to "scan and remove adware from your computer for free." *(See Exhibit A-14, which are true and correct images of the browser window.)*

17. Next, I clicked on the orange "Download" button. A "File Download" window appeared asking whether I wanted to Open or Save the file "uninstaller_exe.php from www.mypctuneup.com." *(See Exhibit A-15, which is a true and correct image of the browser window and File Download window.)*

18. I clicked on the "Save" button, and the "Save As" window appeared. I instructed that the MyPCUninstaller file to be saved to the computer desktop. *(See Exhibit A-16, which is a true and correct image of the browser window and "Save As" window.)*

19. After clicking on the "Save" button, the download process was initiated. Within moments, the download window indicated that the download was complete. *(See Exhibit A-17, which is a true and correct image of the browser window and download window.)*

20. As instructed, I closed the download window by clicking on the "Close" button. I then closed all other browser windows by clicking on the "X" in the top right corner of each window. The desktop showed that the MyPCUninstaller icon had been added to the icons displayed. *(See Exhibit A-18, which is a true and correct image of the desktop.)*

21. Finally, I double-clicked on the MyPCUninstaller icon in an effort to uninstall Aurora. An error message immediately appeared indicating that MyPCUninstaller was "not a valid Win32 Application." *(See Exhibit A-19, which is a true and correct image of the desktop and error message.)*

LyricAndSongs.com: "Browser Enhancement Installation" Download

22. On August 3, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, NY. I ran scans for existing spyware on the computer's hard drive, using the programs Ad-Aware SE Personal Edition and Spybot Search & Destroy. At that time, the programs indicated the hard drive to be free of spyware. (*See Exhibit B-1, which are true and correct images of the result screens.*)

23. I opened the C:\Program Files folder to view a listing of the seventeen files located within that folder. *(See Exhibit B-2, which is a true and correct image of the window.*)

24. I next opened Internet Explorer and the <www.msn.com> start page appeared. *(See Exhibit B-3, which is a true and correct image of the browser window.)*

25. In the address bar, I typed the website address <www.google.com> and the Google search engine appeared. I entered "usher lyrics"[5] into the Google search bar and pressed the enter key. *(See Exhibit B-4, which is a true and correct image of the browser window.)*

26. I scrolled through the first page of search results and clicked on the "2" link at the bottom of the page to be directed to the second page of search results. *(See Exhibit B-5, which is a true and correct image of the Google results.)*

27. I clicked on the link "Lyrics - usher - All songs, words of songs FREE, At lyrics and songs -" and was directed to <www.lyricsandsongs.com/lyrics/USHER.html>. Upon landing at this web page, a pop-up window was immediately displayed titled "Browser Enhancement Installation." The window advertised "a free browser enhancement . . . available to be installed on your system free of charge," and stated that "By installing our software, you agree to the terms

[5] Usher is a popular R&B recording artist.

and conditions stated here." However, no "terms and conditions" were listed, nor was there even a hyperlink to a web site hosting any terms and conditions. This pop-up did not make any mention of any bundled spyware programs. *(See Exhibit B-6, which is a true and correct image of the browser and pop-up window.)*

28. In an effort to close the "Browser Enhancement Installation" pop-up, I simultaneously pressed the Ctrl, Alt and Delete keys. The simultaneous depression of these keys prompted the appearance of the Windows Task Manager. "Browser Enhancement Installation" was listed among the applications running at that time. *(See Exhibit B-7, which is a true and correct image of the Task Manager.)*

29. I selected the "Browser Enhancement Installation" application and then clicked the button marked "End Task." At this time the pop-up window disappeared and I proceeded to close the remaining browser windows by clicking on the "X" in the top right-hand corner of each browser window. I opened Internet Explorer and immediately received a pop-up advertisement generated by Direct Revenue's Aurora Program. *(See Exhibit B-8, which is a true and correct image of the browser window.)*

30. I opened the C:\Program Files folder for a listing of the files located within that folder. This listing indicated that twelve folders had been added during the "Browser Enhancement Installation" download process: AdDestroyer, asys, AutoUpdate, Bullseye Network, Cas, CashBack, CasStub, CMAPP, NaviSearch, Save, SurfSideKick3 and VBouncer. Direct Revenue's Aurora program was not listed. (*See Exhibit B-9, which are true and correct images of the window.*)

31. I closed the C:\Program Files folder and proceeded to the C:\WINDOWS

directory. Twenty-eight additional files had been added to the directory since the "Browser Enhancement Installation" download, including the Direct Revenue files "AuroraHandler.dll," "Nail," "svcproc," and "acvuxrodyad." The listed "Date Modified" for each of the files was June 25, 2001; January 24, 2002; February 26, 2005; and May 8, 2002, respectively. *(See Exhibit B-10, which are true and correct images of the window.)*

32. I closed the C:\WINDOWS directory and launched the Add/Remove utility through the Windows Control Panel. The utility offered the option to change or remove AdDestroyer, CashBackBuddy, LAN Bridge, NaviSearch, SaveNow, Select CashBack, Surf SideKick, Sysnet, The BullsEye Network, Virtual Bouncer, Windows AFA Internet Enhancement and the Windows VisFX Components. Although there was no listing for Aurora, there was a listing for "The ABI Network - A Division of Direct Revenue." *(See Exhibit B-11, which is a true and correct image of the window.)*

33. I closed the Add/Remove utility and ran a scan for existing spyware on the computer's hard drive using Ad-Aware SE Personal Edition. The scan identified 573 objects, including 63 VX2 registry keys, files and folders. (*See Exhibit B-12, which are true and correct images of the scan results.*)

34. I then attempted to run a scan for existing spyware on the unit's hard drive using Spybot Search & Destroy. I was unable to complete the scan due to an "Error during check!" *(See Exhibit B-13, which is a true and correct image of the scan results.)*

35. I logged onto the same undercover computer once again on August 4, 2005. I launched the Add/Remove utility through the Windows Control Panel and was offered the option to change or remove "The ABI Network - A Division of Direct Revenue," which was still listed

among the currently installed programs. *(See Exhibit B-14, which is a true and correct image of the window.)*

36. I clicked on the button marked "Change/Remove" and I was immediately directed to an Internet Explorer browser window with the directory path C:\WINDOWS\abiuninst.htm displayed in the address bar of the browser window. This window directed me to go to the website <www.mypctuneup.com> to remove the "the ABI Network software." *(See Exhibit B-15, which is a true and correct image of the browser window.)*

37. Following the instructions provided, I copied the URL <www.mypctuneup.com> from the displayed text and entered it into the address bar by using the "paste" function. I was then directed to the MyPCTuneUp homepage. *(See Exhibit B-16, which are true and correct images of the browser window.)*

38. I then clicked on the button marked "Uninstall" located on the left side of the browser window and was directed to <www.mypctuneup.com/evaluate.php>, a web page providing instructions to "scan and remove adware from your computer for free." *(See Exhibit B-17, which are true and correct images of the browser window.)*

39. Next, I clicked on the orange "Download" button. A "File Download" window appeared asking whether I wanted to Open or Save the file "uninstaller_exe.php from www.mypctuneup.com." *(See Exhibit B-18, which is a true and correct image of the browser window and File Download window.)*

40. I clicked on the "Save" button and the "Save As" window appeared. I instructed that the MyPCUninstaller file to be saved to the computer desktop. *(See Exhibit B-19, which is a true and correct image of the browser window and "Save As" window.)*

41. After clicking on the "Save" button, the download process was initiated. Within moments, the download window indicated that the download was complete. *(See Exhibit B-20, which is a true and correct image of the browser window and download window.)*

42. As instructed, I closed the download window by clicking on the "Close" button. I then closed all other browser windows by clicking on the "X" in the top right corner of each window. The desktop was now visible and the MyPCUninstaller icon had been added to the icons displayed. *(See Exhibit B-21, which is a true and correct image of the desktop.)*

43. Finally I double-clicked on the MyPCUninstaller in an effort to uninstall Aurora. An error message immediately appeared indicating that MyPCUninstaller was "not a valid Win32 Application." *(See Exhibit B-22, which is a true and correct image of the desktop and error message.)*

LyricAndSongs.com: "Free Browser Enhancement" Download

44. On August 5, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, NY. I ran scans for existing spyware on the computer's hard drive, using the programs Ad-Aware SE Personal Edition and Spybot Search & Destroy. At that time, the programs indicated the hard drive to be free of spyware. (*See Exhibit C-1, which are true and correct images of the result screens.*)

45. I opened the C:\Program Files folder to view a listing of the seventeen files located within that folder. *(See Exhibit C-2, which is a true and correct image of the window.*)

46. I next opened Internet Explorer and the <www.msn.com> start page appeared. *(See Exhibit C-3, which is a true and correct image of the browser window.)*

47. In the address bar, I typed the website address <www.google.com> and the

Google search engine appeared. I entered "usher lyrics" into the Google search bar and pressed enter. *(See Exhibit C-4, which is a true and correct image of the browser window.)*

48. I scrolled through the first page of search results and then clicked on the "4" link at the bottom of the page to be directed to the fourth page of search results. *(See Exhibit C-5, which is a true and correct image of the Google results.)*

49. I clicked on the link "Lyrics - usher - All songs, words of songs FREE, At lyrics and songs -" and was directed to <www.lyricsandsongs.com/lyrics/USHER/html>. Upon landing at this web page, an ActiveX dialog was immediately displayed. The dialog advertised "Free Browser Enhancements" distributed by "Pacerd, Ltd," and made no mention of any bundled spyware programs.

50. In an effort to successfully close the ActiveX dialog and accept the "Free Browser Enhancements," I selected the button marked "Yes." The dialog disappeared and I proceeded to close the remaining browser window by clicking on the "X" in its top right corner. Although all browser windows were closed, I immediately received an Aurora pop-up ad for an internet gambling service. *(See Exhibit C-6 which is a true and correct image of the pop-up window.)*

51. I opened the C:\Program Files folder for a listing of the files located within that folder. This listing indicated that eleven folders had been added as a result of the Pacerd browser enhancement download: AdDestroyer, asys, AutoUpdate, Bullseye Network, Cas, CashBack, CasStub, CMAPP, NaviSearch, SurfSidKick3 and VBouncer. Direct Revenue's Aurora program was not listed. (*See Exhibit C-7, which is a true and correct image of the window.*)

52. I closed the C:\Program Files folder and proceeded to the C:\WINDOWS directory. Thirty-two additional files had been added to the directory since the Pacerd browser

enhancement download including the Direct Revenue files "AuroraHandler.dll," "Nail," "svcproc," and "wszxjsvpdl." The listed "Date Modified" for each of the files was July 11, 2001; July 15, 2000; January 30, 2003; and July 16, 2002, respectively. *(See Exhibit C-8, which are true and correct images of the window.)*

53. I closed the C:\WINDOWS directory and launched the Add/Remove utility through the Windows Control Panel. The utility offered the option to change or remove AdDestroyer, CashBackBuddy, LAN Bridge, NaviSearch, Select CashBack, Surf SideKick, Sysnet, The BullsEye Network, Virtual Bouncer, Windows AFA Internet Enhancement and the Windows VisFX Components. Although there was no listing for Aurora, there was a listing for "The ABI Network - A Division of Direct Revenue." *(See Exhibit C-9, which is a true and correct image of the window.)*

54. I closed Add/Remove and ran a scan for existing spyware on the computer's hard drive using Ad-Aware SE Personal Edition. The scan identified 542 objects, including 67 VX2 registry keys, files and folders. (*See Exhibit C-10, which are true and correct images of the scan results.*)

55. I then attempted to run a scan for existing spyware on the unit's hard drive using Spybot Search & Destroy. I was unable to complete the scan due to an "Error during check!" *(See Exhibit C-11, which is a true and correct image of the scan results.)*

56. I closed Spybot Search & Destroy and proceeded to open Internet Explorer and the <www.msn.com> start page appeared. *(See Exhibit C-12, which is a true and correct image of the browser window.)*

57. In the address bar, I typed the series of random letters "hjgkfhkgvl." Upon my

depression of the enter key, I was directed to a web page titled "Error Page Assistant." The address bar displayed the URL of the "Error Page Assistant" as <http://dr.webservicehosts.com/index.php?tpid=10217&ttid=105&dst=2&st=hjgkfhkgvl&mid=219_3> . Other than the "dr" in the web address, the page contained no information linking it to Direct Revenue or Aurora. *(See Exhibit C-13, which is a true and correct image of the "Error Page Assistant" window.)*

58. At no point during this test was I notified that the standard 404 response or "Not Found" error message would be reset to or replaced by the "Error Page Assistant."

I declare under penalty of perjury that the forgoing is true and correct.

Executed on March __, 2006.

_____

Joseph Rivela
Investigator
New York State Office of the Attorney General
Internet Bureau
120 Broadway
New York, NY 10271

Sworn to before me
this____day of March 2006.

_____

_____Karen Geduldig
_____Notary Public