AFFIDAVIT OF SIBU THOMAS

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

I, Sibu Thomas, 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 February 2005. 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 May 2005 and July 2005, I conducted a number of investigative tests, through Attorney General 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.

Bollywood4U.com: "FlashTalk" Program Download

3. On May 05, 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 & Destroy.[2] At that time,

[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.

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 eighteen files located within that folder. (*See Exhibit A-2, which is a true and correct image of the window.*)

5. I next opened the C:\WINDOWS folder to view a listing of the files located within that folder. (*See Exhibit A-3, which are true and correct images of the windows.*)

6. I next opened Internet Explorer and the <www.msn.com> start page appeared. (*See Exhibit A-4, which is a true and correct image of the browser window.*)

7. In the address bar, I typed the website address <www.bollywood4u.com>. Upon browsing through the website, and the various image galleries located within, an ActiveX dialog offering the installation of "FlashTalk" appeared on the screen. An empty browser window also opened at this time. The ActiveX dialog indicated that the software was distributed by "BetterInternet." The dialog indicated that clicking "Yes" would acknowledge the acceptance and understanding of BetterInternet's "Consumer Policy Agreement." However, the location of this agreement was not indicated, nor was it necessary to read anything prior to proceeding with the installation. The ActiveX dialog made no mention of Direct Revenue's bundled spyware programs. (*See Exhibit A-5, which is a true and correct image of the browser window and ActiveX dialog 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. Many Spybot scans generate five entries for "DSO Exploit" which is not indicative of any resident spyware programs.

8. I clicked on the "Yes" button, indicating my intent to install and run the FlashTalk program. The dialog disappeared, while the aforementioned empty browser window remained in view. I was next guided through three installation screens to set up the FlashTalk program. Again, there was no mention of Direct Revenue's bundled spyware programs. When the installer program indicated that the installation was complete, I clicked on the "Finish" button to exit the installation. (*See Exhibit A-6, which are true and correct images of the browser windows and dialogs.*)

9. Upon exiting the installation program, a "FlashTalk" dialog appeared on the screen, which displayed a "welcome" message. An additional browser window was also visible, which was titled "Download Complete." Clicking "Next" under the welcome message led to a "FLASHTALK LICENSE AGREEMENT" dialog. (*See Exhibit A-7, which are true and correct images of the browser windows and dialogs.*)

10. I clicked the "Accept" button in the aforementioned window, which led to the display of a message indicating that the program was attempting to access the Internet. A message, asking whether I already possessed a FlashTalk account, appeared within the same dialog window. Upon clicking "No," a request for an e-mail address appeared. I attempted to advance without providing this information, by clicking on the "Next" button, but a pop-up window appeared and insisted that I enter the requested data. (*See Exhibit A-8, which are true and correct images of the browser windows and dialogs.*)

11. I clicked "OK" to close the pop-up window, and provided an e-mail address as requested. A pop-up window then appeared, stating that the supplied e-mail address must be valid in order for FlashTalk to operate. I clicked "Yes" to continue. Additional information was

then requested, including a password. I entered the required information and clicked "Next" to proceed. A dialog window then appeared, indicating some of the uses and features of the FlashTalk program. I clicked on the "X" in the top right-hand corner of the window, to dismiss the dialog. The FlashTalk console then appeared, indicating that the program was ready for use. None of the screens I had seen during the installation of FlashTalk had made any mention of Direct Revenue's bundled spyware program. (*See Exhibit A-9, which are true and correct images of the browser windows and dialogs.*)

12. I then minimized the FlashTalk application, and closed all visible browser windows. I opened the C:\Program Files folder for a listing of the files located within that folder. This listing indicated that one new folder had been added during the software download process: FlashTalk. Direct Revenue's Ceres program was not listed. (*See Exhibit A-10, which is a true and correct image of the window.*)

13. I closed the C:\Program Files folder and proceeded to the C:\WINDOWS directory. Four additional files were added to the directory since the installation of FlashTalk, including the Direct Revenue files "ceres.dll" and "farmmext." (*See Exhibit A-11, which are true and correct images of the directory.*)

14. I exited the C:\WINDOWS directory and ran a scan for existing spyware on the computer's hard drive using Ad-Aware SE Personal Edition. The scan identified 70 objects, including many VX2[3] registry keys, files, and a folder. (*See Exhibit A-12, which are true and correct images of the relevant scan results.*)

---

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

15. I opened Internet Explorer at this time, which was set to load <www.msn.com>. Upon loading the aforementioned page, a pop-up window was loaded. The window was titled "Ceres," and displayed an ad for "free Registry Cleaner software" by SysTweak.com. (*See Exhibit A-13, which is a true and correct image of the browser and pop-up windows.*)

16. I then ran a scan for existing spyware on the unit's hard drive using Spybot Search & Destroy. That scan identified 12 "problems," including entries for AbetterInternet[4] and CallingHome.biz.[5] (*See Exhibit A-14, which are true and correct images of the relevant scan results.*)

17. I closed Spybot – Search & Destroy and reopened Internet Explorer. Immediately, another "Ceres" pop-up ad appeared, offering "free Registry Cleaner software" by SysTweak.com. (*See Exhibit A-15, which is a true and correct image of the browser and pop-up windows.*)

18. I closed the "Ceres" pop-up ad, and remained at the MSN.com website. Without any further input, a second pop-up appeared. This pop-up window displayed an ad for <www.888.com>, an online casino and poker room site. (*See Exhibit A-16, which is a true and correct image of the browser and pop-up windows.*)

19. I then closed all the windows and restarted the unit. At that time, I opened Internet Explorer and directed it to <www.cnn.com>. I received a Ceres pop-up ad for

---

[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."

[5] CallingHome.biz was an early web domain used by Direct Revenue in conducting its spyware business. Spybot Search & Destroy often identifies Direct Revenue spyware files as "CallingHome.biz."

"ConsumerIncentivePromotions." (*See Exhibit A-17, which is a true and correct image of the browser and pop-up windows.*)

20. Finally, I proceeded to the "Add or Remove Programs" control panel, and viewed a listing of the programs that were installed on the hard drive at that time. There was no listing for Direct Revenue's spyware program. (*See Exhibit A-18, which is a true and correct image of the control panel window.*)

IOWRESTLING.com: "FlashTalk" Program Download

21. On May 10, 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.*)

22. 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.*)

23. I next opened the C:\WINDOWS folder to view a listing of the files located within that folder. (*See Exhibit B-3, which are true and correct images of the windows.*)

24. I then opened Internet Explorer and the <www.msn.com> start page appeared. (*See Exhibit B-4, which is a true and correct image of the browser window.*)

25. In the address bar, I typed the website address <www.iowrestling.com>. Upon browsing through the website, and the various sections located within, an ActiveX dialog box offering the installation of "FlashTalk" appeared on the screen. An empty browser window also appeared at that time. The ActiveX dialog indicated that the software was distributed by

"BetterInternet." The dialog indicated that clicking "Yes" would acknowledge the acceptance and understanding of BetterInternet's "Consumer Policy Agreement." However, the location of this agreement was not indicated, nor was it necessary to read anything prior to proceeding with the installation. The ActiveX dialog made no mention of Direct Revenue's bundled spyware program. (*See Exhibit B-5, which is a true and correct image of the browser and ActiveX dialog windows.*)

26. I clicked on the "Yes" button, indicating my agreement to install and run the FlashTalk installation. The dialog disappeared, while the aforementioned empty browser window remained in view. I was next guided through three installation screens to set up the FlashTalk program. Again, there was no mention of Direct Revenue's bundled spyware programs. I clicked on the "Finish" button to exit the installation. (*See Exhibit B-6, which are true and correct images of the browser windows and dialogs.*)

27. Upon exiting the installation program, a "FlashTalk" dialog appeared on the screen, which displayed a "welcome" message. An additional browser window was also visible, which was titled "Download Complete." Clicking "Next" under the welcome message led to a "FLASHTALK LICENSE AGREEMENT" dialog. (*See Exhibit B-7, which are true and correct images of the browser windows and dialogs.*)

28. I clicked the "Accept" button in the aforementioned window, which led to the display of a message indicating that the program was attempting to access the Internet. A message, asking whether I already possessed a FlashTalk account, appeared within the same dialog window. I proceeded to the next screens, where information such as e-mail address, name, and password were requested. The required information was entered at that time. I

clicked next to proceed. Next, I received a request for the e-mail address of friends who might want to use FlashTalk. I clicked next to proceed without entering any e-mail addresses. (*See Exhibit B-8, which are true and correct images of the browser windows and dialogs.*)

29. A dialog window then appeared, indicating some of the uses and features of the FlashTalk program. I clicked on the "X" in the top right-hand corner of the window, to dismiss the dialog. The FlashTalk console then appeared, indicating that the program was ready for use. None of the many screens I had seen during the installation of FlashTalk had made any mention of Direct Revenue's bundled spyware programs. (*See Exhibit B-9, which are true and correct images of the browser windows and dialogs.*)

30. I then minimized the FlashTalk application, and closed all visible browser windows. I opened the C:\Program Files folder for a listing of the files located within that folder. This listing indicated that one new folder had been added during the software download process: FlashTalk. Direct Revenue's Ceres program was not listed. (*See Exhibit B-10, which is a true and correct image of the window.*)

31. I closed the C:\Program Files folder and proceeded to the C:\WINDOWS directory. Thirteen additional files had been added since the installation of FlashTalk, including the Direct Revenue files "ceres.dll" and "farmmext." (*See Exhibit B-11, which are true and correct images of the directory.*)

32. I opened Internet Explorer at this time, which was set to load <www.msn.com>. Upon loading the aforementioned page, a pop-up window was loaded. The window was titled as "Ceres," and displayed an advertisement for "ConsumerIncentivePromotions." (*See Exhibit B-12, which is a true and correct image of the browser and pop-up windows.*)

33. I exited Internet Explorer and ran a scan for existing spyware on the computer's hard drive using Ad-Aware SE Personal Edition. The scan identified 142 objects, including many VX2 registry keys and values, files, a running process and a folder. Files identified as VX2 components, ekwwwkod.exe and payload2.inf, had been identified in the C:\Windows\System32 and C:\Windows\inf directories respectively. (*See Exhibit B-13, which are true and correct images of the relevant scan results.*)

34. I then ran a scan for existing spyware on the unit's hard drive using Spybot Search & Destroy. That scan identified 42 "problems," including entries for AbetterInternet and CallingHome.biz. (*See Exhibit B-14, which are true and correct images of the relevant scan results.*)

35. I proceeded to the "Add or Remove Programs" control panel, and viewed a listing of the programs that were installed on the hard drive at that time. There was no listing for Direct Revenue's spyware program. (*See Exhibit B-15, which is a true and correct image of the control panel window.*)

36. I then closed all open programs, and later re-opened Internet Explorer. A "Ceres" pop-up window appeared upon the loading of the MSN home page. This pop-up window displayed an advertisement for "free Registry Cleaner software" by SysTweak.com. (*See Exhibit B-16, which is a true and correct image of the browser and pop-up windows.*)

37. I returned to the machine after a day and reopened Internet Explorer. Upon browsing various websites such as MSN, Yahoo, and Google's search engine, I received a number of Ceres pop-ups. When three Ceres pop-ups had appeared on the screen, they were grouped on the taskbar into one entry listed as "Buddy." (*See Exhibit B-17, which are true and*

correct images of the browser and pop-up windows.)

38. I entered the URL <mypctuneup.com> into the address bar of the web browser. I was then directed to the MyPCTuneUp homepage. 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-18, which are true and correct images of the browser windows.*)

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 mypctuneup.com." (*See Exhibit B-19, which is a true and correct image of the browser and "file download" windows.*)

40. I clicked on the "Save" button and the "Save As" window appeared. I instructed that the MyPCUninstaller file be saved to the computer desktop. (*See Exhibit B-20, which is a true and correct image of the browser and "Save As" windows.*)

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-21, which is a true and correct image of the browser and download windows.*)

42. As instructed, I closed the download window by clicking on the "Close" button. I then closed all windows but the main browser window by clicking on the "X" in the top right corner of each window. The desktop was now visible and indicated that the MyPCUninstall icon had been added to the icons displayed. (*See Exhibit B-22, which is a true and correct image of the desktop.*)

43. Finally, I double-clicked on the MyPCUninstall icon located on the desktop. At that time, a window appeared indicating that the program would "remove all advertising software produced by our affiliates from your computer." (*See Exhibit B-23, which is a true and correct image of the window.*)

44. I clicked "Next" to proceed to the next screen. I was then prompted to enter a randomly generated security code to proceed with the uninstall. I entered this code and clicked "Submit." (*See Exhibit B-24, which is a true and correct image of the window.*)

45. A message appeared indicating that the code was verified, and that the uninstall process could be continued. I clicked on the "Delete" button to proceed with the process. (*See Exhibit B-25, which is a true and correct image of the window.*)

46. The window then displayed a message indicating that the uninstall was completed. Upon clicking the "Finish" button, another message appeared indicating that the computer must be restarted in order to complete uninstallation. I clicked on "Yes" to restart the machine. (*See Exhibit B-26, which is a true and correct image of the window.*)

47. I proceeded to search for files labeled "Ceres" located on the C:\ drive. The search led to a folder found at C:\Documents and Settings\Melissa\Local Settings\Temp\DrTemp. This folder contained several Direct Revenue files, including the ceres.dll and farmmext files previously identified. (*See Exhibit B-27, which is a true and correct image of the window.*)

700xxx.com: "Aurora" Download

48. On May 13, 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 before visiting the website. This was accomplished by 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 abovementioned program results.*)

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

50. I next opened the C:\Windows folder to view the listing of the files located within that folder. (*See Exhibit C-3, which are true and correct images of the windows.*)

51. I then opened Internet Explorer and the <www.msn.com> start page appeared. (*See Exhibit C-4, which is a true and correct image of the browser window.*)

52. In the address bar, I typed the website address <www.700xxx.com>. Upon clicking on one of the thumbnail photographs, a dialog indicating a download for "Java virtual machine" appeared on the screen. Before any interaction could take place, much of the screen became inaccessible and the computer ceased to respond. (*See Exhibit C-5, which are true and correct images of the browser and dialog windows.*)

53. After approximately one minute, the browser window and the aforementioned dialog disappeared from the screen. An Internet Explorer error, as well as an error dialog for "Web Site Viewer" appeared. Two other error dialogs soon appeared on the screen. (*See Exhibit C-6, which are true and correct images of the dialog windows.*)

54. After dismissing the various errors, I then ran a scan for existing spyware on the computer's hard drive using Ad-Aware SE Personal Edition. The scan identified 600 objects, including many VX2 registry keys, values, files, and a folder. (*See Exhibit C-7, which are true and correct images of the relevant scan results.*)

55. I exited Ad-Aware SE Personal Edition and ran a scan for existing spyware on the unit's hard drive using Spybot Search & Destroy. That scan identified 133 "problems," including entries for AbetterInternet and CallingHome.biz. (*See Exhibit C-8, which are true and correct images of the relevant scan results.*)

56. I then opened Internet Explorer, which was set to load <www.msn.com>. Upon visiting <www.msnbc.com>, a pop-up window was loaded. The window was titled "Aurora," and displayed an ad for an online casino and poker room called "www.888.com". (*See Exhibit C-9, which is a true and correct image of the browser and pop-up windows.*)

57. Upon visiting other websites, such as <www.news.com> and <www.wired.com>, additional "Aurora" pop-up windows appeared. These pop-ups displayed advertisements for companies such as Cingular, Sprint, T-Mobile, Tickle, and GoToMyPC. (*See Exhibit C-10, which are true and correct images of the browser and pop-up windows.*)

58. I then proceeded to the C:\Program Files directory to view a listing of the files located within that folder. At that time, several new folders were found. Direct Revenue's Aurora program was not listed. (*See Exhibit C-11, which is a true and correct image of the windows.*)

59. I next opened the C:\WINDOWS directory to view a listing of the files located within that folder. New files had been installed since visiting 700xxx.com, including the Direct Revenue files "svcproc," "Nail," and "ucpvyttbvvt." The listed "Date Modified" for each of the files was April 18, 2003; June 2, 2004; and October 27, 2001, respectively. (*See Exhibit C-12, which are true and correct images of the windows.*)

UKBritney.tv: "Pacerd" Browser Enhancements Download

60. On May 23, 2005, I logged on to the internet using an undercover computer located at 120 Broadway, New York, NY. I ran scans for existing spyware on the computer's hard drive before visiting the website. This was accomplished by 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 D-1, which are true and correct images of the abovementioned program results.*)

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

62. I next opened the C:\WINDOWS folder to view the listing of the files located within that folder. (*See Exhibit D-3, which are true and correct images of the windows.*)

63. I then opened Internet Explorer and the <www.msn.com> start page appeared. (*See Exhibit D-4, which is a true and correct image browser window.*)

64. In the address bar, I typed the website address <www.ukbritney.tv>. Upon browsing through the main page of the website, an ActiveX dialog box offering the installation of "Free Browser Enhancements" appeared on the screen. An empty browser window also opened at this time. The ActiveX dialog indicated that the software was distributed by "Pacerd, Ltd." The ActiveX dialog made no mention of Direct Revenue's bundled spyware program. (*See Exhibit D-5, which are true and correct images of the browser and ActiveX dialog windows.*)

65. I clicked on the blue text in the ActiveX box, which led to a "PACERD MEDIA END USER LICENSE AGREEMENT." The agreement made no mention of Direct Revenue's bundled spyware programs. (*See Exhibit D-6, which are true and correct images of the browser*

windows.)

66. I clicked on the "Yes" button, indicating my agreement to install and run the installation of "Free Browser Enhancements." The dialog disappeared, while the aforementioned empty browser window remained in view. I proceeded to close two of the four open windows, and opened a new browser window. At that time, an "Aurora" pop-up ad appeared on the screen. This window displayed an ad for "free Registry Cleaner software" by SysTweak.com. (*See Exhibit D-7, which is a true and correct image of the browser and pop-up windows.*)

67. I then closed all the open windows and returned to the machine after some time. Upon opening Internet Explorer, an "Aurora" pop-up immediately appeared again with an advertisement for <www.888.com>. (*See Exhibit D-8, which is a true and correct image of the browser and pop-up windows.*)

68. I closed the aforementioned windows and then proceeded to the "Add or Remove Programs" control panel, and viewed a listing of the programs that were installed on the hard drive at that time. Direct Revenue's Aurora program was not listed. (*See Exhibit D-9, which is a true and correct image of the window.*)

69. I opened the C:\Program Files folder for a listing of the files located within that folder. This listing indicated that six new folders had been added during the installation process: AdDestroyer, AutoUpdate, FwBarTemp, Toolbar, Vbouncer, WeirdOnTheWeb. Direct Revenue's Aurora program was not listed. (*See Exhibit D-10, which is a true and correct image of the window.*)

70. I closed C:\Program Files and proceeded to the C:\WINDOWS directory for a listing of the files located within that folder. This listing indicated that several new files had

been added during the installation process, including the Direct Revenue files "svcproc," "Nail," and "jhvramslo." The listed "Date Modified" for each of the files was June 21, 2004; July 31, 2002; and July 7, 2004, respectively. (*See Exhibit D-11, which are true and correct images of the window.*)

71. I exited the C:\WINDOWS directory and ran a scan for existing spyware on the computer's hard drive using Ad-Aware SE Personal Edition. The scan identified 697 objects, including many VX2 registry keys, files, and a folder. (*See Exhibit D-12, which are true and correct images of the relevant scan results.*)

72. I then ran a scan for existing spyware on the unit's hard drive using Spybot Search & Destroy. That scan identified 144 "problems," including entries for AbetterInternet. (*See Exhibit D-13, which is a true and correct image of the relevant scan results.*)

UKBritney.tv: "Aurora" Download - Security: Low

73. On May 23, 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 E-1, which are true and correct images of the abovementioned program results*.)

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

75. I next opened the C:\WINDOWS folder to view the listing of the files located within that folder. (*See Exhibit E-3, which are true and correct images of the window(s).*)

76. I then opened Internet Explorer and the <www.msn.com> start page appeared.

(*See Exhibit E-4, which is a true and correct image browser window.*)

77. Next, I proceeded to the "Tools" menu in Internet Explorer, and clicked on "Internet Options." I then clicked on the "Security" tab and changed the security level to "Low." (*See Exhibit E-5, which is a true and correct image of the browser and options windows.*)

78. In the address bar, I typed the website address <www.ukbritney.tv>. Upon browsing through the main page of the website, I received two dialog boxes requesting permission to install software from 180solutions and Web Search Tools. I declined to consent to both installations. (*See Exhibit E-6, which are true and correct images of the browser windows.*)

79. I then opened a new Internet Explorer window and proceeded to <www.msn.com>. I clicked on a link for a news article in the MSNBC subsection. As soon as the page started to load, I received an Aurora pop-up window. The window displayed an ad for Registry Cleaner software, offered by SysTweak.com. (*See Exhibit E-7, which is a true and correct image of the browser and pop-up windows.*)

80. I closed the aforementioned pop-up window and proceeded to <www.google.com>. I initiated a search for the term "spyware," and was immediately presented with an Aurora pop-up ad for "@mazing search." This window displayed search results for the term that I had entered into Google's search engine. (*See Exhibit E-8, which is a true and correct image of the browser and pop-up windows.*)

81. While browsing through various sites, I repeatedly received Aurora pop-up ads for various sites such as Pacific Poker, PartyPoker.com, Vegas Splendido Online Casino, and <www.888.com>. (*See Exhibit E-9, which are true and correct images of the browser and pop-up windows.*)

82. I closed all of the aforementioned browser and pop-up windows. I opened the "Add or Remove Programs" control panel, and viewed a listing of the programs that were installed on the hard drive at that time. Direct Revenue's Aurora program was not listed. (*See Exhibit E-10, which is a true and correct image of the control panel window.*)

83. I proceeded to the C:\Program Files folder for a listing of the files located within that folder. The listing indicated that two new folders had been added during the installation process: "Internet Optimizer" and "joystick networks." Direct Revenue's Aurora program was not listed. (*See Exhibit E-11, which is a true and correct image of the window.*)

84. I closed C:\Program Files and proceeded to the C:\WINDOWS directory for a listing of the files located within that folder. Several files had been added during the installation process, including the Direct Revenue Files "svcproc," "Nail," and "qqyzxzzeo." The listed "Date Modified" for each of the files was June 16, 2001; November 22, 2004; and May 25, 2003, respectively. (*See Exhibit E-12, which are true and correct images of the window.*)

85. I exited the C:\WINDOWS directory and ran a scan for existing spyware on the computer's hard drive using Ad-Aware SE Personal Edition. The scan identified 201 objects, including many VX2 registry keys, files, and a folder. *(See Exhibit E-13, which are true and correct images of the relevant scan results.*)

86. I then ran a scan for existing spyware on the unit's hard drive using Spybot Search & Destroy. That scan identified 79 "problems," including entries for AbetterInternet. (*See Exhibit E-14, which is a true and correct image of the relevant scan results.*)

IOWRESTLING.com: "FreePhone" Program Download

87. On May 27, 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 F-1, which are true and correct images of the result screens.*)

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

89. I next opened the C:\WINDOWS folder to view a listing of the files located within that folder. (*See Exhibit F-3, which are true and correct images of the windows.*)

90. I proceeded to the "Add or Remove Programs" control panel, and viewed a listing of the programs that were installed on the hard drive at that time. (*See Exhibit F-4, which is a true and correct image of the control panel window.*)

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

92. In the address bar, I typed the website address <www.iowrestling.com>. Upon browsing through the website, and the various sections located within, an ActiveX dialog box offering the installation of "FreePhone Installer" appeared on the screen. An empty browser window also appeared at that time. The ActiveX box indicated that the software was distributed by "BetterInternet." The dialog indicated that clicking "Yes" would acknowledge the acceptance and understanding of BetterInternet's "Consumer Policy Agreement." However, the location of the agreement was not indicated, nor was it necessary to read anything prior to proceeding with the installation. (*See Exhibit F-6, which is a true and correct image of the browser and ActiveX dialog windows.*)

93. I then clicked on the text that stated the above mentioned information. This link directed the browser to the "BETTERINTERNET END USER LICENSE AGREEMENT," which was contained in 20 full-size screens. (*See Exhibit F-7, which are true and correct images of the browser window(s).*)

94. I closed the browser window containing the license agreement. I then clicked the "Yes" button on the ActiveX box, indicating my intent to install and run the FreePhone Installer. Within a matter of minutes, a "FreePhone" dialog appeared on the screen. This dialog indicated that the program was attempting to access the internet, and asked if I already have a "FreePhone account." (*See Exhibit F-8, which is a true and correct image of the browser and dialog windows.*)

95. I clicked on the button labeled "No Create a New Account." The dialog then displayed a request for a name and password. The required information was entered at that time, and I then clicked "Next". (*See Exhibit F-9, which is a true and correct image of the browser and dialog windows.*)

96. The FreePhone console then appeared on the screen, indicating that the program was ready for use. (*See Exhibit F-10, which is a true and correct image of the browser and console window.*)

97. I then minimized the FreePhone application and proceeded to open a new Internet Explorer window, which was set to load <www.msn.com>. An "Aurora" pop-up window appeared once the MSN home page was loaded. This pop-up window displayed an advertisement for an "Internet Security Update" from SoftwareOnline.com. (*See Exhibit F-11, which is a true and correct image of the browser and pop-up windows.*)

98. I opened the C:\Program Files directory for a listing of the files located within that folder. This listing indicated that one new folder had been added during the software download process: FreePhone. Direct Revenue's Aurora program was not listed. (*See Exhibit F-12, which is a true and correct image of the window.*)

99. I closed the C:\Program Files folder and proceeded to the C:\WINDOWS directory. Additional files had been added to the directory since the installation of FreePhone, including the Direct Revenue files "svcproc," "Nail," and "qmglburgm." The "Date Modified" for each of the files was March 20, 2005; October 20, 2003; and July 4, 2002, respectively. (*See Exhibit F-13, which are true and correct images of the directory.*)

100. I exited the C:\WINDOWS directory and proceeded to the "Add or Remove Programs" control panel. Although there was no entry for Aurora, there was an entry for "The ABI Network - A Division of Direct Revenue." (*See Exhibit F-14, which is a true and correct image of the control panel window.*)

101. I then ran a scan for existing spyware on the computer's hard drive using Ad-Aware SE Personal Edition. The scan identified 52 objects, including many VX2 registry keys and values, files, a running process and a folder. (*See Exhibit F-15, which are true and correct images of the relevant scan results.*)

102. I then ran a scan for existing spyware on the unit's hard drive using Spybot Search & Destroy. That scan identified 9 "problems," including entries for AbetterInternet. (*See Exhibit F-16, which is a true and correct image of the relevant scan results.*)

103. I then proceeded to conduct searches in Internet Explorer, using the Google search engine located at <www.google.com>. Upon conducting a search for "online gambling", an

Aurora pop-up window appeared. This pop-up window displayed an advertisement for "@mazing search," with several links to various online gambling and resource sites. (*See Exhibit F-17, which is a true and correct image of the browser and pop-up windows.*)

104. I re-directed the browser to <www.microsoft.com>. Upon loading this page, an Aurora pop-up window appeared. This pop-up window displayed an advertisement for "WinAntiVirusPro 2005" stating "Your Current Antivirus Protection is Not Effective!" (*See Exhibit F-18, which is a true and correct image of the browser and pop-up windows.*)

105. I entered <www.msnbc.com> to proceed to the MSNBC home page. As soon as the page had completed loading, an Aurora pop-up window appeared. This pop-up window displayed an advertisement for an "Internet Security Update" from SoftwareOnline.com. (*See Exhibit F-19, which is a true and correct image of the browser and pop-up windows.*)

EBS.FUCK-ACCESS.COM: "Aurora" Download

106. On June 14, 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 G-1, which are true and correct images of the result screens.*)

107. I opened the "Add or Remove Programs" control panel, and viewed a listing of the programs that were installed on the hard drive at that time. (*See Exhibit G-2, which is a true and correct image of the control panel window.*)

108. I opened the C:\Program Files folder to view a listing of the seventeen files located within that folder. (*See Exhibit G-3, which is a true and correct image of the window.*)

109. I next opened the C:\WINDOWS folder to view a listing of the files located within that folder. (*See Exhibit G-4, which are true and correct images of the windows.*)

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

111. In the address bar, I typed the website address <www.ebs.fuck-access.com>. Upon depressing the "enter" key, an "Install on Demand (Other)" dialog appeared on the screen, as well as an error indicating that problems with the website might prevent viewing it properly. Both windows were dismissed by clicking on the "X" in the top right-hand corners (*See Exhibit G-6, which is a true and correct image of the browser window.*)

112. I then went to the "Tools" menu, chose "Options," and proceeded to the "Security" tab. The security settings for Internet Explorer had been set to "Low" upon entering the URL for the ebs.fuck-access.com website. (*See Exhibit G-7, which is a true and correct image of the browser window.*)

113. The computer ceased to respond to any further input. After a couple of minutes, the browser window was minimized and an "Aurora" pop-up window appeared. This pop-up displayed an advertisement for "Registry Cleaner," promising "Tools to Safely clean and repair Windows," "Fewer Computer and Internet Freezes," and "Fewer Computer Crashes." (*See Exhibit G-8, which is a true and correct image of the browser and pop-up window.*)

114. I opened the "Add or Remove Programs" control panel and noted that several new programs had been installed: Internet Optimizer, ISTsvc, Maxifiles, Media-motor, SpySheriff, Surf SideKick, and UCMore - The Search Accelerator. Although there was no entry for Aurora, there was an entry for "The ABI Network - A Division of Direct Revenue." (*See Exhibit G-9,*

which is a true and correct image of the control panel window.)

115. I then opened the C:\Program Files directory to view a listing of the files located within that folder. Several new folders had been added. Direct Revenue's Aurora program was not listed. (*See Exhibit G-10, which are true and correct images of the windows.*)

116. I proceeded to the C:\WINDOWS directory to view a listing of the files located within that folder. Several files had been added, including the Direct Revenue files "svcproc," "Nail," and "hhqbijwqy." The listed "Date Modified" for each of the files was October 18, 2001; June 9, 2000; and April 25, 2004, respectively. (*See Exhibit G-11, which are true and correct images of the windows.*)

117. I ran a scan for existing spyware on the computer's hard drive using Ad-Aware SE Personal Edition. The scan identified 359 objects, including several VX2 registry keys and values, files, a folder, and a running process. (*See Exhibit G-12, which are true and correct images of the relevant result screens.*)

118. I then ran a scan for existing spyware on the computer's hard drive using Spybot Search & Destroy. That scan identified 90 "problems," including entries for AbetterInternet and CallingHome.biz. (*See Exhibit G-13, which is a true and correct image of the relevant result screens.*)

119. I proceeded to open Internet Explorer. Upon loading the MSN home page, an Aurora pop-up was loaded. The pop-up displayed an ad for an "Internet Security Scan" from SoftwareOnline.com. (*See Exhibit G-14, which is a true and correct image of the browser and pop-up window.*)

120. All windows were then closed, and the machine was left in a secured state until

June 30, 2005. Upon accessing the desktop, numerous Internet Explorer windows had been opened without any interaction. In addition to this, three "Aurora" pop-up windows had appeared. The pop-up windows were arranged under one taskbar entry, titled "Buddy." These pop-up windows (one of which was empty) displayed ads for AdultFriendFinder.com, as well as "Registry Cleaner" by SysTweak.com. (*See Exhibit G-15, which are true and correct images of the browser and pop-up windows.*)

IEPrivacy.com: Program Download

121. On June 24, 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 H-1, which are true and correct images of the result screens.*)

122. I opened the "Add or Remove Programs" control panel, and viewed a listing of the programs that were installed on the hard drive at that time. (*See Exhibit H-2, which is a true and correct image of the control panel window.*)

123. I next opened the C:\Program Files directory to view a listing of the seventeen files located within that folder. (*See Exhibit H-3, which is a true and correct image of the window.*)

124. I then proceeded to the C:\WINDOWS directory to view a listing of the files located within that folder. (*See Exhibit H-4, which are true and correct images of the window(s).*)

125. I then opened Internet Explorer and the <www.msn.com> start page appeared.

(*See Exhibit H-5, which is a true and correct image of the browser window.*)

126. In the address bar, I typed the website address <www.ieprivacy.com>. This page advertised and described IEPrivacy's privacy protection software. However, the page contained no diclosure about or reference to Direct Revenue's bundled spyware programs. I clicked on a link on the left side of the page titled "Click Here Free Download." (*See Exhibit H-6, which are true and correct images of the browser windows.*)

127. The page <www.ieprivacy.com/download.html> was loaded in the window. The page displayed an example of an ActiveX dialog window, and advised the user to click "Yes" when the dialog box appeared. The message also indicated that it was a "free and safe" download, certified by Microsoft Authenticode. (*See Exhibit H-7, which is a true and correct image of the browser window.*)

128. Although no ActiveX box appeared, two "File Download" windows popped up on the screen, indicating that the file "IEPrivacy-install.exe" was being downloaded. The window also provided the option of opening or saving the file. I clicked on the "open" option to proceed without saving the file to the hard drive. *(See Exhibit H-8, which is a true and correct image of the browser and dialog windows.*)

129. An "IEPrivacy Installer Setup Wizard" interface then appeared on the screen to guide me through the installation of IEPrivacy. I clicked "Next" to proceed with the installation. (*See Exhibit H-9, which is a true and correct image of the dialog window.*)

130. The install wizard then displayed a license agreement. This license agreement was contained over 188 small screens that could not be expanded. On the 131st screen, I came to a section titled "BETTERINTERNET END USER LICENSE AGREEMENT." I scrolled

through the agreement and clicked on the "I Agree" button. (*See Exhibit H-10, which is a true and correct image of the dialog/agreement window.*)

131. Within moments, the install wizard displayed a message which indicated that the IEPrivacy Installer had been installed on the computer. I clicked on the "Finish" button to exit the installer. (*See Exhibit H-11, which is a true and correct image of the dialog window.*)

132. At that time, a window titled "IEPrivacy2" appeared on the screen. In the background, two browser windows appeared indicating that "WebSearch Toolbar" had been sucessfully installed. A small blue icon appeared in the taskbar tray, matching the logo displayed on the aforementioned WebSearch Toolbar page. (*See Exhibit H-12, which is a true and correct image of the program and browser windows.*)

133. I then closed the aforementioned windows and opened a new Internet Explorer window. I proceeded to <www.google.com> to conduct a search. I entered the term "spyware," and viewed the results provided. At that time, a pop-up window titled "Ceres" appeared on the screen. This pop-up displayed an advertisement for a ringtone of Gwen Stefani's "Rich Girl," by WannaBeHeard.com. (*See Exhibit H-13, which is a true and correct image of the browser and pop-up windows.*)

134. I then closed the abovementioned browser window. After several minutes, an Internet Explorer window appeared, along with a "Ceres" pop-up window displaying the same advertisement as discussed supra. (*See Exhibit H-14, which is a true and correct image of the browser and pop-up windows.*)

135. Once again, I closed all Internet Explorer windows. Without any interaction, a pop-up window titled "Aurora" appeared on the screen. This pop-up window displayed an

advertisement for a free "The Game" ringtone, by WannaBeHeard.com. (*See Exhibit H-15, which is a true and correct image of the pop-up window.*)

136. I opened the C:\Program Files directory for a listing of the files located within that folder. This listing indicated that nine new folders had been added during the software download process: AutoUpdate, bsaa, eZula, IEPrivacy, SurfSideKick 3, Toolbar, Vbouncer, Web_Rebates, and WeirdOnTheWeb. Direct Revenue's Aurora program was not listed. (*See Exhibit H-16, which is a true and correct image of the window.*)

137. I closed the C:\Program Files folder and proceeded to the C:\WINDOWS directory to view a listing of the files located within that folder. Several files had been added during the software download process, including the Direct Revenue files "svcproc," "Nail," and "cxyxdleinm." The "Date Modified" listed for each of the files was April 25, 2004; June 19, 2004; and October 6, 2002, respectively. (*See Exhibit H-17, which are true and correct images of the windows.*)

138. I ran a scan for existing spyware on the computer's hard drive using Ad-Aware SE Personal Edition. The scan identified 709 objects, including numerous VX2 registry keys, registry values, and files. (*See Exhibit H-18, which are true and correct images of the relevant result screens.*)

139. I then ran a scan for existing spyware on the computer's hard drive using Spybot Search & Destroy. That scan identified 218 "problems," including entries for AbetterInternet. (*See Exhibit H-19, which is a true and correct image of the relevant result screens.*)

140. I proceeded to open Internet Explorer, which was set to load <www.msn.com>. I then entered <www.google.com> into the location bar, and pressed "Enter". As soon as the key

was depressed, an Aurora pop-up window appeared on the screen. This pop-up window displayed an advertisement for Overstock.com. (*See Exhibit H-20, which is a true and correct image of the browser and pop-up window.*)

141. I closed the above mentioned windows, and proceeded to the "Add/Remove Programs" control panel. Several new programs were listed, including: Content Delivery Module, Display Utility, IEPrivacy, InternetOffers, OIN, Search Assistant, TSA, WebRebates (by TopRebates.com), WebSearch Toolbar, WeirdOnTheWeb, and Windows AFA Internet Enhancement. Although Aurora was not listed, there was an entry for "The ABI Network - A Division of Direct Revenue." (*See Exhibit H-21, which is a true and correct image of the control panel window.*)

AbetterInternet.com: Archived Site Images:

142. On July 15, 2005, I logged onto the internet from an undercover computer located at 120 Broadway, New York, NY. I then opened Internet Explorer and directed the browser to <www.archive.org>. On this page, I proceeded to the section for the "Wayback Machine" and entered <www.abetterinternet.com>. I then clicked on the "Take Me Back" option to proceed to a list of archived dates for the aforementioned site.

143. I clicked on the link for "June 02, 2004." I browsed through the main page, and then proceeded to click on the link for "NetTurbo," which would purportedly "optimize your connection to the Internet with 200%." At that time, an ActiveX box appeared on the screen. I clicked on the blue text in the ActiveX box, which led me to the Consumer Policy Agreement. (*See Exhibit I-1, which are true and correct images of the browser and ActiveX box windows.*)

144. I returned to the list of archived dates at Archive.org. I clicked on July 16, 2004

and browsed through the main page. I then clicked on the link for Eliminate Spam, "a free anti-spam software." At that time, an ActiveX box appeared on the screen. I clicked on the blue text in the ActiveX box, which led me to the Consumer Policy Agreement. (*See Exhibit I-2, which are true and correct images of the browser and ActiveX box windows.*)

145. I then returned to the abovementioned list of dates and chose October 30, 2004. I browsed through the main page and proceeded to click on the link for Atomic Clock, a program that "will always be in sync with the US Government Atomic Clock!" An ActiveX box appeared on the screen, and I clicked on the blue text in the ActiveX box in order to proceed to the Consumer Policy Agreement. However, the link to the agreement was unavailable at that time. (*See Exhibit I-3, which are true and correct images of the browser and ActiveX windows.*)

146. I returned to the list of dates and proceeded to November 27, 2004. I clicked on the link for Clean Get-Away, which led to a new install window prompting me to accept the "ActiveX Control." I clicked "No" in the ActiveX box, declining the installation. (*See Exhibit I-4, which is a true and correct image of the browser and ActiveX windows.*)

147. Next, I clicked on the "more info" link for Clean Get-Away, and then clicked on the "EULA" link on that page. The aforementioned link led to a "BETTERINTERNET END USER LICENSE AGREEMENT." (*See Exhibit I-5, which are true and correct images of the browser windows.*)

148. Finally, I returned to the list of dates and chose "September 25, 2004." I scrolled through the page, and clicked on the link for "More Downloads." On the Downloads page, I proceeded to click on the link for "Mahjong." At this time, a new install window appeared prompting me to accept the "ActiveX Control." I clicked "No" in the ActiveX box, declining the

installation. (*See Exhibit I-6, which is a true and correct image of the browser and ActiveX windows.*)

Blubster.com: End-User License Agreement

149. On March 23, 2006, I logged onto the internet from an undercover computer located at 120 Broadway, New York, NY. I then opened Internet Explorer and directed the browser to <www.blubster.com>. (*See Exhibit J-1, which is a true and correct image of the browser window.*)

150. On the aforementioned page, I clicked on the link for "free download." At that time, a "File Download" window appeared requesting that I open or save "blubstersetup250.exe." I clicked "Save" and proceeded to save the file to the Desktop. *(See Exhibit J-2, which are true and correct images of the windows.*)

151. Shortly after clicking "Save," a window displayed the download process and then indicated that the download was complete. I clicked on "Open" to launch the Blubster 2.5 setup program. *(See Exhibit J-3, which are true and correct images of the download windows.*)

152. The Blubster 2.5 Setup window then appeared. I clicked on "Next" to proceed with the installation. An "End User License Agreement" was displayed in the window. This license agreement contained 79 screens that could not be expanded. I scrolled through the agreement and clicked on the "Accept" button. (*See Exhibit J-4, which are true and correct images of the program/agreement windows.*)

153. The program then requested a "Destination Location." I accepted the default directory and clicked "Next." An install window then appeared and later indicated that "Blubster 2.5 has been successfully installed." (*See Exhibit J-5, which are true and correct images of the*

program windows.)

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

Executed on March __, 2006

Sibu Thomas
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