### RECEIVED

#### UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF ILLINOIS EASTERN DIVISION

SEP 1 3 2005

MICHAEL W. DOBBINS
CLERK, U.S. DISTRICT COURT

LOGAN SIMIOS, individually and on behalf of all persons similarly situated,	)		
Plaintiff,	)		
v.	)	Case No. 05C	5235
180SOLUTIONS, INC. and		JURY DEMANDED	0200
JOHN DOES 1-100	) )	JUDGE ASPEN	
Defendants.	<b>5</b>	MAGISTRATE JUDGE NOLAN	

#### **CLASS ACTION COMPLAINT**

Plaintiff, Logan Simios, individually, and on behalf of all persons similarly situated, by and through his attorneys, for his Complaint against Defendants, states and alleges as follows:

#### Introduction

1. 180Solutions has unlawfully used and damaged Plaintiff's computer to make money for itself, while willfully disregarding Plaintiff's rights to use and enjoy his personal property.

Defendants deceptively downloaded harmful and offensive "spyware" to Plaintiff's computer. The spyware tracked Plaintiff's Internet use, invaded his privacy, and damaged his computer. Relying on spyware as the key to getting inside Plaintiff's computer and learning his Internet browsing habits, 180Solutions invaded Plaintiff's privacy and interfered with Plaintiff's right to use and enjoy his computer. The putative Classes in this case have been violated and damaged in the same ways.

Plaintiff brings this action to enjoin Defendants' unlawful misconduct, to seek compensation for the damage caused, and to seek certification of Classes of those similarly situated.

#### **Parties**

- 2. Plaintiff Logan Simios is a citizen of the state of Illinois and this Judicial District.
- 3. 180Solutions, Inc. is incorporated in both Washington and New York. 180Solutions' principal place of business is in Bellevue, Washington. 180Solutions, thus, is a citizen of the states of New York and Washington.
- 4. John Does 1-100 represent the individual employees, officers, agents, distributors and advertisers who assisted in the misconduct alleged herein and/or who displayed their advertisements on computers. When their identities are ascertained, they will also be named as Defendants.

#### Jurisdiction and Venue

- 5. This Court has personal jurisdiction over 180Solutions and venue is proper in this Judicial District because this case arises out of actions which occurred, at least in part, within this Judicial District including, *inter alia*:
- (a) 180Solutions causes its spyware to be downloaded onto computers in this Judicial District and its spyware damages computers located in this Judicial District.
- (b) 180Solutions has infected over 20 million computers and has business relationships with more than 6,000 advertisers including dozens of Fortune 1000 companies. Upon information and belief, at least hundreds of thousands of the infected computers and dozens (if not hundreds) of these advertisers are located within this Judicial District.
- 6. Pursuant to the Class Actions Fairness Act of 2005, this Court has subject matter jurisdiction to hear the pending claims because the amount in controversy exceeds \$5,000,000 and members of the putative Plaintiff Class are from different states than 180Solutions.

- 7. Subject matter jurisdiction is also appropriate because Plaintiff has brought Federal claims pursuant to the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA") and the Electronic Communications Privacy Act, 18 U.S.C. § 2707, 2511, 2520 ("ECPA").
- 8. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because they arise out of the same common nucleus of operative fact as Plaintiff's Federal claims and would ordinarily be expected to be tried in one judicial proceeding.

#### **Allegations of Fact**

#### "Spyware"

- 9. As used herein, "spyware" describes computer software downloaded to an end-user's computer over the Internet, without consent, that permits the company which downloaded the software (i.e., the spyware company) to track, profile, and analyze a computer user's behavior, for the purpose of sending him or her targeted advertising, which the spyware company can place for its "clients".
- 10. 180Solutions boasts in marketing literature that it is able to provide advertisers with "a 360-degree view of the user's behavior -- 24 hours a day, 7 days a week." For example, if a computer infected with 180Solutions' spyware is browsing/viewing music-related Internet sites, the spyware sends a signal of such activity back to 180Solutions, which then targets the computer user with advertisements from competing music companies who have paid for access to these computers via the unlawfully-installed spyware. Likewise, if a computer user types in a search phrase (i.e., "Maui hotels") into a search engine (such as Google), 180Solutions intercepts

There are many different definitions of "spyware" according to Google.com, including: (1) "also known as 'adware', [i]t is a hidden software program that transmits user information via the Internet to advertisers in exchange for free downloaded software." (2) "Software that tracks usage and reports it to others, such as advertisers. Usually the tracking is concealed from the user of the software."

the search and sends an advertisement on behalf of one of its customers (such as a hotel in Maui) that paid 180Soloutions to monitor the searches performed by computer users.

#### 180Solutions' Rusiness Model

- 11. 180Solutions pays its distributors, who are its agents, money each time they infect a computer with 180Solutions' spyware. These infections occur over the Internet on various sites such as those offering games and music. 180Solutions recruits distributors, at least in part, through unsolicited spam emails.
- 12. In a 2004 interview with the <u>Los Angeles Times</u>, a 180Solutions senior employee characterized distributors as: "guys in Bermuda, offshore. They're the online equivalent of spammers" and he further admitted that 180Solutions "had not been careful enough in overseeing" such companies.
- 13. 180Solutions currently has its spyware installed on approximately 20,000,000 computers.
- 14. The reason 180Solutions infects computers with spyware is because once the spyware is installed, advertisers pay 180Solutions to spy on the Internet sites visited by computer users and to send targeted advertising to them.

#### 180Solutions' Illegal Practices

- 15. 180Solutions deceptively distributes its spyware files (deceptively referred to as, *interalia*, "nCase") and prevents users from removing the files once installed.
- 16. For example, the <u>Los Angeles Times</u> has reported that "180Solutions programs have been installed through Microsoft security holes" and further that:
  - "180's program, nCase, is notorious in the antispyware community both for the amount of advertisements it sends to individual computers (hundreds per day) and its near impossibility to remove. Many spyware programs, like nCase, hide themselves so well they can't be removed even if found by standard uninstall features of Microsoft Windows."

- 17. 180Solutions engages in uniformly deceptive misconduct to download its spyware. This is how it's done: 180Solutions and its agents bundle spyware into other legitimate software which is available to be downloaded for "free" on the Internet. For example, a computer user may find a supposedly "free" software program on the Internet, such as a video game. When the computer user downloads and installs that "free" game, he or she simultaneously (but unknowingly) downloads 180Solutions spyware, since it was bundled into the game being downloaded.
- 18. A March 2005 study of 180Solutions by Sunbelt Software<sup>2</sup> concluded that:

180 seems unable or unwilling to rein in distributors ("partners") who resort to unethical means of presenting 180's software to users and even installing it on users' PCs through security exploits in order to get paid for those installations.

\*\*\*

Given the functionality of 180 solutions' software as well as its checkered distribution history -- a history which includes rampant "force-installs" of 180's software on users' PCs without those users' full knowledge and consent -- the anti-spyware community is entirely justified in being skeptical of 180's claims to have reformed its software and distribution practices.

- 19. Computer users do not consent, let alone have knowledge, that spyware is being installed on their computers. This is because 180Solutions has deceptively caused its spyware to download without consent or knowledge through deceptive methods including, *inter alia*, automatic installations, viruses, and through exploiting security deficiencies in Microsoft's Internet Explorer. In all of these methods, computer users are not told of, or even given the opportunity to stop, spyware infections.
- 20. 180Solutions' spyware is also deceptively distributed with other spyware from other companies. For example, on many occasions, 180Solutions' spyware is co-bundled with

<sup>&</sup>lt;sup>2</sup> Sunbelt Software is a leading international software company that studies spyware. It offers products to protect and secure computer systems from spyware and spam and undertook a detailed 56 page study of 180Solutions' software in March 2005.

spyware from DirectRevenue, another spyware company. Thus, a computer is infected with spyware from both companies in the same way. DirectRevenue's spyware distribution practices are the subject of a pending lawsuit in this Judicial District, *Sotelo v. DirectRevenue*, et al, 05-CV-2562.

#### 180Solutions Lies to Consumers about its spyware.

21. 180Solutions lies to computer users about its spyware. For instance, 180Solutions displays the following message to computer users about its "software":



22. The above advertisement is false. 180Solutions software does contain spyware, it does hide on a computer so that it cannot be easily detected, it does invade privacy by monitoring Internet sites visited, and it shares data with others by allowing third parties to reap the benefit of targeted advertisements by providing them "a 360-degree view of the user's behavior -- 24 hours a day, 7 days a week."

#### Once installed, 180Solutions deceptively prevents users from removing its spyware.

- 23. After the deceptive installation of its spyware, 180Solutions then engages in a uniformly deceptive course of conduct to prevent users from removing the spyware after it is installed. Former employees of 180Solutions have reported that 180Solutions makes the process to uninstall its spyware "intentionally difficult for consumers."
- 24. 180Solutions also falsely tells consumers that if its spyware is removed, other software on the user's computer will not operate.
- 25. 180Solutions markets its spyware under various names, often having no apparent relationship to 180Solutions so that users cannot figure out how to complain about the spyware

or to remove it. Upon information and belief, the various misleading file names used by 180Solutions include, *inter alia*, msbb.exe, saie.exe, salm.exe, saap.exe, sain.exe, zango.exe, and nCase/md.

26. 180Solutions utilizes a "resuscitator" program that is installed by 180Solutions' spyware into Microsoft directory of files. This program is randomly named and designed to avoid detection by anti-spyware applications. Moreover, the sole purpose of this program is to monitor the installed 180Solutions' spyware and scare a user to reinstall the spyware files should they be removed. For example, 180Solutions causes a "WARNING" to appear that tells computer users that removing its spyware "may cause some programs not to run as expected".

#### Damage Caused by Defendants' Unlawful Conduct

- 27. 180Solutions' spyware causes computers to slow down, takes up bandwidth over an Internet connection, uses up memory on a computer, utilizes pixels and screen-space on monitors, causes the loss of data, and frustrates computer users. Defendants' spyware and popup advertisements decrease productivity by requiring that hours be spent figuring out how to get them off of a computer, closing advertising windows, and waiting for a slower machine to operate. Furthermore, computer users are forced to keep their computers running longer (due to the slowed performance) which utilizes more electricity, decreases the useful life of a computer, and causes increased Internet access charges. The cumulative impact of not only multiple ads, but also the threat of future ads and monitoring, impedes computer usage. The cost to purchase software to effectively remove spyware, unwanted advertisements, and guard against future infections is approximately \$30 per year per computer.
- 28. Indeed, in its State of Spyware report for 2005, Webroot Software, Inc. (a leading international software company) reported as one of the Internet's "Top Threats" for spyware,

180Solutions' spyware and noted that it may "send information about your Web surfing habits to its controlling servers whenever you are online, which may slow your Web browser's performance [and] may download third-party programs on your computer, resulting in unwanted programs being installed without your knowledge or consent."

#### Named Plaintiff Allegations

29. 180Solutions infected Logan Simios' computer with spyware during 2005. The spyware was installed without any notice and without the opportunity to consent. As a result of the spyware installations, Logan Simios' computer has been damaged as alleged above.

#### Class Allegations

- 30. Plaintiff brings each of the claims in this action in his own name and on behalf of a class of all persons similarly situated ("the Class") pursuant to Federal Rule of Civil Procedure 23.
- 31. This case is brought on behalf of two Classes. The Class definitions are as follows:
  - <u>Class "A"</u> "All persons and entities in the United States who had 180Solutions' spyware installed on their computers, in or after September 12, 2002."
  - Class "B" "All persons and entities in Illinois who had 180Solutions' spyware installed on their computers, in or after September 12, 2002."
- 32. Plaintiff is a member of each Class. The Class is so numerous that joinder of all members is impractical. Upon information and belief, there are approximately 20,000,000 affected computers. Upon information and belief, Class A has many million Class members, and Class B has at least hundreds of thousands of Class members.
- 33. There are questions of law and fact which are common to the Class which predominate over any questions affecting only individual members, including:
  - a. Whether Defendants engaged in deceptive business practices in causing spyware to be downloaded onto the computers of the members of Class A and Class B;

- b. Whether Defendants' above alleged conduct violates the Computer Fraud and Abuse Act;
- c. Whether the Electronic Communications Privacy Act applies to spyware installations and monitoring;
- d. Whether Defendants have committed a trespass to chattels;
- e. Whether 180Solutions intended to deceive the members of Class A and Class B into downloading software;
- f. Whether Defendants violated the Illinois Consumer Fraud Act; and
- g. Whether Defendants' conduct in downloading bundled software constitutes Computer Tampering under the Illinois Criminal Code.
- 34. The representative party will fairly and adequately protect the interest of the Class. Plaintiff's claims are typical of the claims of the Class. All are based upon the same factual and legal theories. Plaintiff has retained counsel who is competent and experienced in class litigation.
- 35. The class action is an appropriate method for the fair and efficient adjudication of the controversy. The intentionally deceptive conduct of 180Solutions makes it difficult to sue them, let alone ascertain who they are for a lawsuit. Furthermore, the likely individual recovery would not warrant an individual lawsuit due to the expensive nature of litigation, hiring experts, and paying lawyers.

### Count I Computer Fraud and Abuse Act

(Nationwide Class Sought on behalf of Class A)

- 36. Plaintiff re-alleges paragraphs 1 through 35 as if fully set forth herein.
- 37. The CFAA provides for a cause of action against anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ...

information... if the conduct involved an interstate or foreign communication...". 18 USC § 1030

- 38. 18 USC § 1030(g) provides that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief".
- 39. 180Solutions intentionally accessed Plaintiff's computer and the computers of the members of Class A, without consent, by installing spyware on these computers and by communicating with the computers via advertisements, software updates, and Internet use monitoring once the spyware was installed.
- 40. Plaintiff's computer and the computers of the members of Class A are used in interstate communications and commerce and are protected computers within the meaning of the CFAA.
- 41. Plaintiff and the members of Class A have been damaged as a result as alleged herein. Specifically, by 180Solutions' release of each of its viruses (such as nCase), there has been loss and damage to one or more persons (and specifically to the members of Class A) during each of the past years aggregating well in excess of \$5,000.
- 42. Likewise, 180Solutions' spyware constitutes a threat to public health or safety, namely the safety of the public using the World Wide Web. As a result of spyware, including 180Solutions' "top threat" spyware, reliable and generally accepted statistics now show that 91% of internet users have changed their online behavior for fear of becoming victims of spyware, 81% of internet users say they have stopped opening email attachments unless they are sure these documents are safe, 48% of internet users say they have stopped visiting particular Internet sites that they fear might deposit unwanted programs on their computers, 25% of internet users say they have stopped downloading music or video files from peer-to-peer networks to avoid getting

unwanted software programs on their computers, and 93 million American Internet users (68% of them) have had computer trouble in the past year that is consistent with problems caused spyware and viruses. Spyware is also the reported as one of the leading cause of computer complaints, indeed, one third of Microsoft operating system crashes are a result of spyware. The threat to public safety is growing at alarming rates. The number of spyware distribution sites (such as those used to distribute 180Solutions' spyware) has reportedly quadrupled during 2005 alone according to industry research from Webroot Software, Inc. Finally, the public health and safety is also threatened by 180Solutions' spyware because it was distributed at an Internet site (and thus financially supported an Internet site) showing child pornography.

## Count II Electronic Communications Privacy Act /Wiretap Act (Nationwide Class Sought on behalf of Class A)

- 43. Plaintiff re-alleges paragraphs 1 through 42 as if fully set forth herein.
- 44. The ECPA provides a private right of action against one who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C.A. § 2707 and 2520.
- 45. 180Solutions intentionally and without consent intercepted Plaintiff's and the members of Class A's communications with Internet sites and search engines for tortious purposes, specifically to spy on their private Internet browsing use and to trespass on their computer. At this time, 180Solutions intentionally accessed the spyware that it had placed on these computers in electronic storage. 180Solutions also intentionally used its spyware to intercept communications by Plaintiff and Class A to Internet sites.
- 46. 180Solutions further disclosed to others the content of electronic communications knowing that the communications were illegally obtained.

- 47. 180Solutions collected Plaintiff's personal information and the personal information of the members of Class A without consent or compensation, and to misappropriate personality, thereby obtaining detailed, free market research and consumer analysis rather than paying for it.
- 48. As a result of Defendants' misconduct, Plaintiff and Class A were damaged as alleged herein. Pursuant to Section 2707 of the ECPA, Plaintiff and Class A are entitled to be compensated for their damage, the Defendants' profits, or are entitled to statutory damages of \$1,000 per violation, and punitive damages and attorney fees.

### <u>Count III</u> <u>Trespass to Personal Property/Chattels—Illinois Common Law</u> (Illinois Class Sought on behalf of Class B)

- 49. Plaintiff re-alleges paragraphs 1 through 48 as if fully set forth herein.
- 50. At all times relevant hereto, Plaintiff and the members of Class B were the owners of computers or internet connections that were infected with 180Solutions' spyware.
- 51. At all relevant times, Defendants' and/or their agents intentionally and without consent, used Plaintiff's computer and the computers of Class B and their Internet connections, gained access to their computers, monitored their Internet usage, sent advertisements to these infected computers, accessed various components and systems within these computers, obtained access to information about Plaintiff and the members of Class B and their computers, took up space on these computers, and/or dispossessed Plaintiff and the members of Class B of access to their computers.
- 52. In doing so, Defendants intentionally intermeddled with, damaged, and deprived Plaintiff and Class B of their computers and/or Internet connections, or a portion thereof.

#### Count IV

#### **Illinois Consumer Fraud Act**

(Illinois Class Sought on behalf of Class B)

- 53. Plaintiff re-alleges paragraphs 1 through 52 as if fully set forth herein.
- 54. At all relevant times, there was in full force and effect the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 ("Consumer Fraud Act").
- 55. Section 2 of the Consumer Fraud Act, 815 ILCS 505/2 provides:

Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in Section 2 of the "Uniform Deceptive Trade Practices Act", approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby. In construing this section consideration shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a) of the Federal Trade Commission Act.

- 56. The Consumer Fraud Act incorporates § 2 of the Uniform Deceptive Trade Practices Act by prohibiting "unfair methods of competition and unfair or deceptive acts or practices, including but not limited to ... the use or employment of any practice described in § 2 of the Uniform Deceptive Trade Practices Act."
- 57. The Uniform Deceptive Trade Practices Act, 815 ILCS 510/1, provides in pertinent part, at Section 2:

A person engages in a deceptive trade practice when, in the course of his or her business, vocation, or occupation, the person:

- (1) passes off goods or services as those of another;
- (2) causes likelihood of confusion or of misunderstanding as to the source, sponsorship, approval, or certification of goods or services;

\*\*\*

(9) advertises goods or services with intent not to sell them as advertised;

\*\*\*

- (12) engages in any other conduct which similarly creates a likelihood of confusion or misunderstanding.
- 58. 180Solutions engaged in deceptive and misleading advertisements by downloading its spyware onto computers while computer users thought they were downloading "free" software. This advertising is false because the software is not "free". To the contrary, the spyware gives 180Solutions and its advertisers access to engage in ongoing interference with a computer and subjects the computer user to monitoring. Furthermore, 180Solutions lies to computer users about its spyware.
- 59. By secretly bundling its spyware with that of legitimate software programs such as games and screensavers, 180Solutions is passing off its spyware as goods or services of another.
- 60. 180Solutions has also set up its spyware to intentionally confuse, deceive, and mislead consumers into downloading its software, into keeping the software on a computer once installed, and into purchasing anti-spyware software so the advertisements will stop.
- 61. 180Solutions' software is also misleading in that it makes it difficult to remove its spyware from computers once installed as alleged herein.
- 62. 180Solutions' failure to notify consumers that its spyware damages computers, is difficult to remove from a computer, will slow down and/or damage the performance of a computer, and will result in persistent and distasteful advertising is an omission of material fact in violation of the Consumer Fraud Act.
- 63. 180Solutions intended to profit, and did actually profit, from its wrongful conduct by being able to obtain more adverting money by virtue of being downloaded onto more computers.

- 64. 180Solutions knew that its conduct was deceptive and misleading and intended for consumers to be deceived so they would download spyware along with other legitimate software.

  180Solutions' method of distributing its spyware created and continues to create a substantial likelihood of confusion, deception, and misunderstanding. Such deception occurred in the course of trade and commerce.
- 65. As a direct and proximate cause of 180Solutions' misrepresentations and deception, the damage alleged herein occurred.
- 66. 180Solutions' conduct as alleged herein constitutes an unfair practice because it is unlawful, offends public policy, it is immoral, unethical, oppressive and unscrupulous, and it results in substantial economic injury to consumers.
- 67. Injunctive relief is warranted to stop Defendants' ongoing deceptive conduct and to prevent the ongoing invasion of the privacy of Plaintiff and the members of Class B.

## Count V Negligence—Illinois Common Law (Illinois Class Sought on behalf of Class B)

- 68. Plaintiff re-alleges paragraphs 1 through 67 as if fully set forth herein.
- 69. 180Solutions, having gained access to Plaintiff's computer and the computers of the members of Class B, had a duty not to harm the computers and impact their operation. Furthermore, 180Solutions had a duty to monitor its spyware distributors to assure that they, inter alia, obtained user consent for downloading it spyware.
- 70. 180Solutions breached this duty by damaging Plaintiff's and Class B members' computers and interfering with their operation and by not adequately monitoring its spyware distributors.

71. As a direct and proximate result of 180Solutions' negligence, Plaintiff and the members of Class B were damaged as alleged herein.

### Count VI Computer Tampering - Criminal Code (Illinois Class Sought on behalf of Class B)

- 72. Plaintiff re-alleges paragraphs 1 through 71 as if fully set forth herein.
- 73. Section 16D-3 of the Illinois Criminal Code (720 ILCS 5/16D-3) provides in part:
  - (a) A person commits the offense of computer tampering when he knowingly and without the authorization of a computer's owner, as defined in Section 15-2 of this Code, or in excess of the authority granted to him: \*\*\*
  - (4) Inserts or attempts to insert a "program" into a computer or computer program knowing or having reason to believe that such "program" contains information or commands that will or may damage or destroy that computer, or any other computer subsequently accessing or being accessed by that computer, or that will or may alter, delete or remove a computer program or data from that computer, or any other computer program or data in a computer subsequently accessing or being accessed by that computer, or that will or may cause loss to the users of that computer or the users of a computer which accesses or which is accessed by such "program";
- 74. Defendants' conduct, as alleged herein, violated Section 16(D)(3) and proximately caused the damage alleged herein.
- 75. Section 16(D)(3), provides that:

"Whoever suffers loss by reason of a violation of subsection (a)(4) of this Section may, in a civil action against the violator, obtain appropriate relief. In a civil action under this Section, the court may award to the prevailing party reasonable attorney's fees and other litigation expenses."

# Count VII Invasion of Privacy—Illinois Common Law (Illinois Class Sought on behalf of Class B)

- 76. Plaintiffs re-allege paragraphs 1 through 75 as if fully set forth herein.
- 77. Computers provide users with apparent seclusion, solitude and privacy.

- 78. 180Solutions intentionally intruded upon the solitude and seclusion of Plaintiff and the members of Class B by invading the privacy of computer use through monitoring Internet browsing habits and the personal interests of these computer users.
- 79. The invasion by 180Solutions would be highly offensive to a reasonable person and damaged Plaintiff and the members of Class B.
- 80. Likewise, by selling advertising to third parties based upon the private behavior of Plaintiff and the members of Class B, 180Solutions wrongfully appropriated Plaintiff's and the members of Class B's personality for commercial use.

#### PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for the following relief:

- A. An order certifying Class A and Class B as set forth herein, with Plaintiff as the Class representative of each of these classes and his counsel as Class counsel;
- B. Judgment in favor of Plaintiff, Class A and Class B, and against Defendants and awarding damages in the form of compensatory, punitive, loss of use, diminution in value, loss of enjoyment and use, statutory, and disgorgement of ill-gotten gains;
- C. Injunctive relief enjoining the deceptive and misleading spyware practices, the sending of advertisements, and the damage to computers;
- D. All statutory damages available pursuant to the claims made herein;
- E. An award of reasonable attorneys' fees, costs, and expenses; and
- F. Such further relief as this Court deems just and proper.

#### **Jury Demand**

Plaintiff and the members of Class A and Class B demand a trial by jury on all claims so triable.

DATED: September 13, 2005

Respectfully submitted,

By:

One of Plaintiff's attorneys

Shawn M. Collins David J. Fish THE COLLINS LAW FIRM, P.C. 1770 N. Park Street, Suite 200 Naperville, Illinois 60563 Norman B. Berger Michael D. Hayes VARGA BERGER LEDSKY HAYES & CASEY 224 South Michigan Avenue, Suite 350 Chicago, IL 60604