Mona Sedky Spivack, DC #447968
J. Ronald Brooke, Jr., MD #0202280002

PLAINTIFF

4. Plaintiff, the Federal Trade Commission, is an independent agency of the United States government created by statute. 15 U.S.C. §§ 41 *et seq*. The Commission enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits deceptive or unfair acts or practices in or affecting commerce. The Commission is authorized to initiate federal district court proceedings by its own attorneys to enjoin violations of the FTC Act to secure such equitable relief as may be appropriate in each case, including restitution for injured consumers, consumer redress, and disgorgement. 15 U.S.C. § 53(b).

DEFENDANTS

5. Defendant MaxTheater, Inc. ("MaxTheater") is a Washington corporation with its principal place of business located at 5701 South Hailee Lane, Apt. 131, Spokane, Washington 99223, as well as P.O. Box 30220, Spokane, Washington 99223. Defendant MaxTheater does or has done business as "SpywareAssassin" and "SpywareAssassin.com." Defendant MaxTheater transacts or has transacted business in this District.

6. Defendant Thomas L. Delanoy is or has been an officer and owner of

the defendants make these spyware removal claims when the defendants' "anti-spyware" software fails to remove significant amounts of spyware that resides on a computer.

10. Ultimately, in the course of marketing, selling, and distributing their purported "anti-spyware" software, the defendants make material false and misleading representations in their marketing media and, accordingly, engage in deceptive acts or practices in violation of Section 5 of the FTC Act.

Deceptive Spyware Detection Claims

11. In their marketing media, the defendants define spyware, describe the dangers associated with it, and then claim that they have scanned or otherwise examined the consumer's computer and detected that the consumer's computer already has spyware installed on it.

12. For example, on their web site, www.spywareassassin.com, the defendants warn that "spyware & adware are harmful programs which secretly install on your computer without your permission or knowledge . . . decrease your computers [sic] performance [and cause] the flood of popup ads . . . and is responsible for many harmful ads & tactics, including: pop-ups, banner ads, highjacked search engine

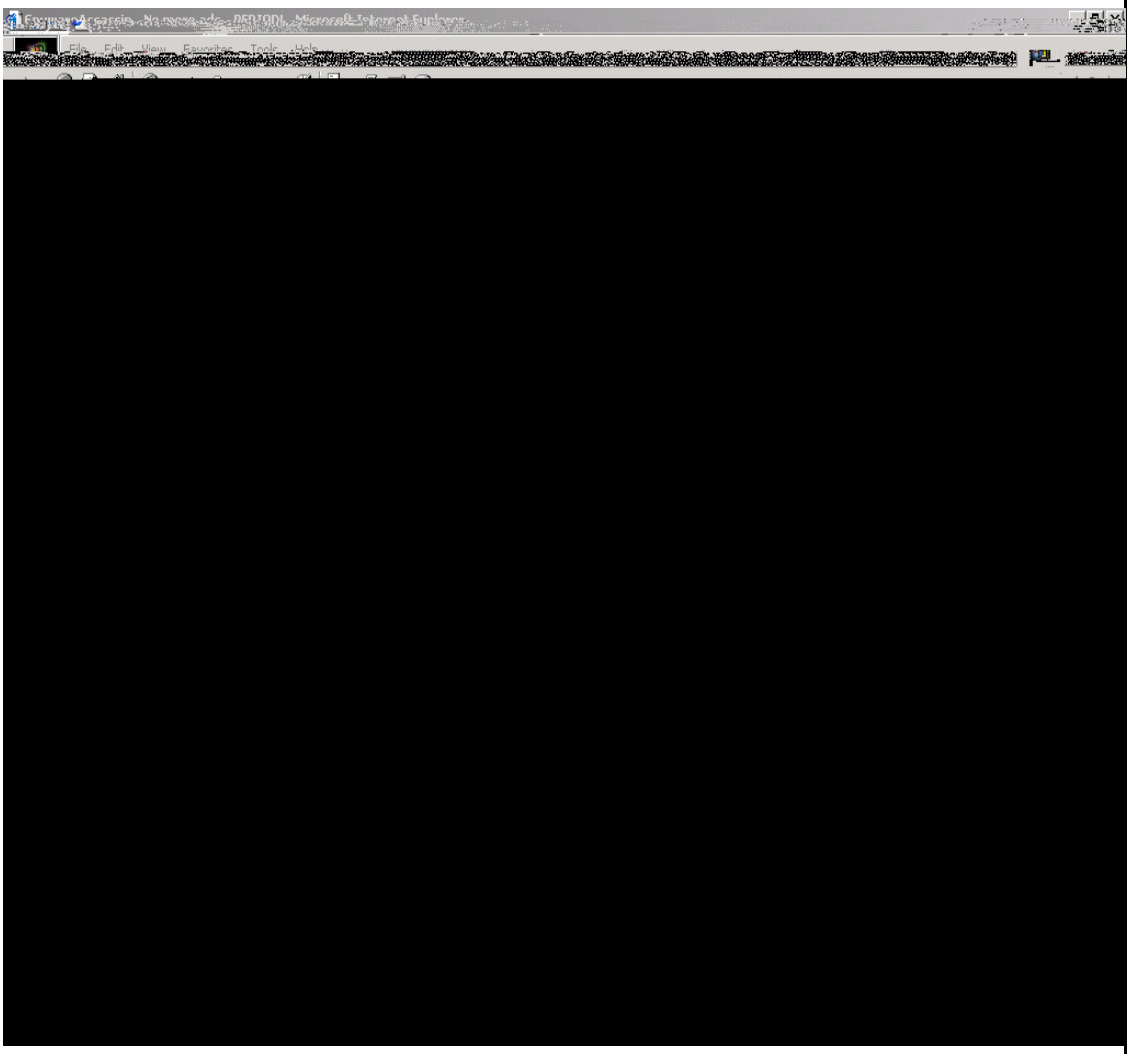
links, hijacked homepages, spam emails, activity tracking, file stealing, credit card theft, fatal Trojan viruses, remote PC access, slow internet connection [that will] ultimately . . . eventually damage your computer so significantly that it will cease from working." The defendants unequivocally state that "if you do not protect your computer from spyware infections **you WILL eventually experience credit card and/or identity theft and your computer will ultimately crash & cease working for good . . . It's not a matter of if, but truly a matter of when.**" (Emphasis in original).

13. In their marketing media, the defendants also purport to perform two types of free spyware scans on consumers' computers. One scan is purportedly performed remotely and is initiated automatically by the defendants when a consumer visits or lands on certain portions of the defendants' web site. The other scan is purportedly performed locally and is initiated by the consumer when the consumer installs and runs the defendants' software product. In either case, the defendants claim that their scans have detected that the consumer's computer already has spyware installed on it.

14. With regard to the defendants' remote spyware scan, the defendants

automatically display a spyware detection “pop up” message that “pops up” on a consumer’s computer screen within seconds after a consumer visits, or lands on certain pages of the defendants’ web site, such as www.spywareassasssin.com/index8.html. In their “pop up” message, the defendants state in bold text: “URGENT ERROR ALERT: You have dangerous spyware virus infections on your computer. Please click OK to install the latest free update to fix these errors. Immediate action is highly recommended before you continue!” Attached as Exhibit A below is a screen-shot of the defendants’ spyware detection “pop up” message:

Exhibit A



15. In numerous instances, the defendants' free remote scan is phony, and the defendants' representations that they have detected spyware on the consumer's computer are deceptive. At the time that the defendants display their initial spyware detection "pop up," the defendants do not

know (and cannot know) whether the consumer's computer in fact already has "spyware" installed on it. At this point, the consumer's computer has not yet been scanned or otherwise examined for spyware. The defendants display their spyware detection "pop up" message automatically, regardless of whether the consumer has clicked on the defendants' "free scan"/download icons or otherwise initiated the defendants' local spyware scan described below. Further, in numerous instances the defendants display their spyware detection "pop up" even when, in fact, the computer is "clean" and does not have spyware installed on it.

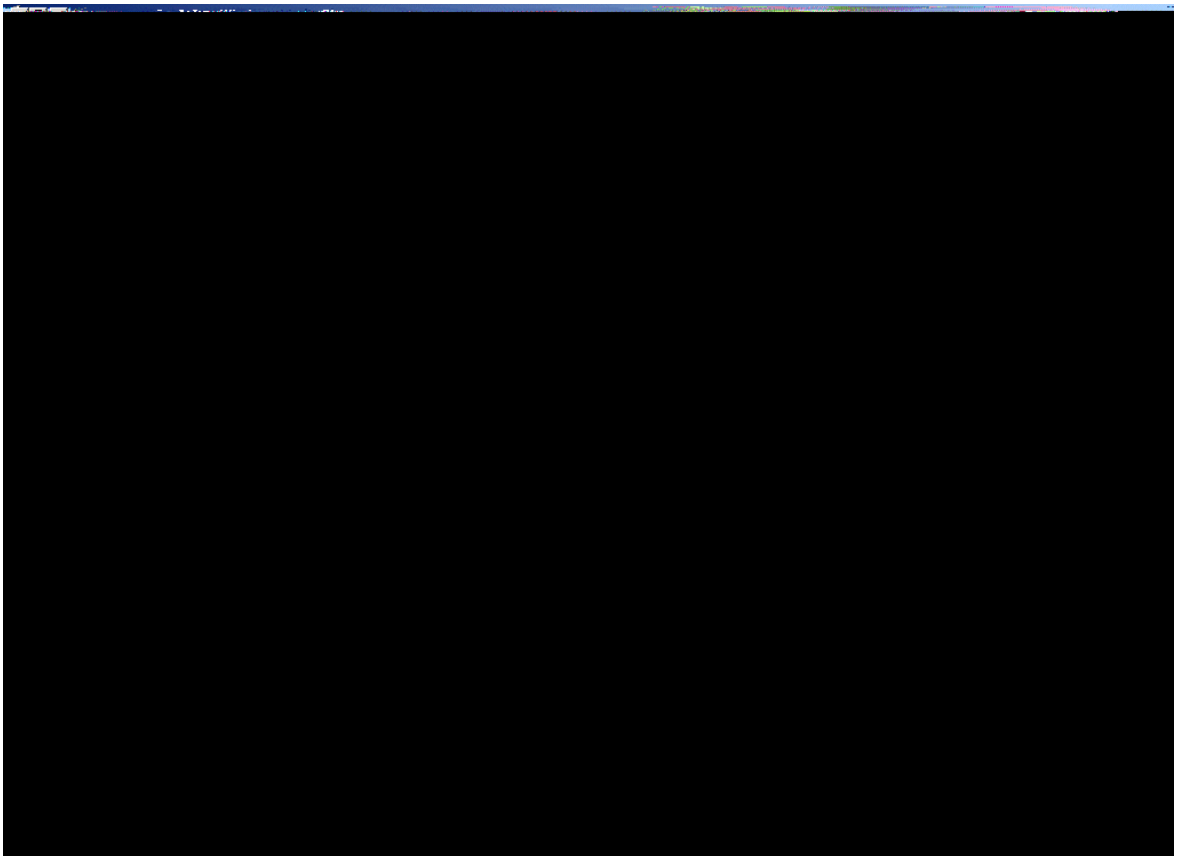
16. With regard to the defendants' free local scan, the defendants state on their web site that "Spyware Assassin . . . will scan your entire system [for] all spyware programs . . . " and "will perform an initial scan, which will locate any and all spyware currently residing on your system . . . ." They display in their marketing media several icons or buttons that are labeled "free scan" and free "demo" or trial download. After a consumer clicks on one of these icons or buttons, the defendants then guide the consumer through a series of steps to download and install the defendants' "anti-spyware" software and to

then run the software to perform the purported spyware scan.

17. During and at the culmination of the defendants' free purported local scan, the defendants repeatedly represent that they have detected spyware on the consumer's computer. For example, while the defendants' local scan is in progress, the defendants display a window on the consumer's computer screen that purports to provide a real-time summary of the results of the scan. These scan results include the quantity and types of spyware detected on the consumer's computer, as well as the location of the file folders (denominated "category" and "value") that contain the detected spyware.

18. In numerous instances, the defendants have stated in their scan results window that their scan has detected several well-known software programs installed on a computer, including, but not limited to, "Gator," "Bargain Buddy," "Xupiter," and "Flash Track." The defendants have also identified the location of the purported spyware, listing several file folder names next to each of the identified pieces of spyware. Attached as Exhibit B below is a screen-shot of the defendants' scanning window:

Exhibit B



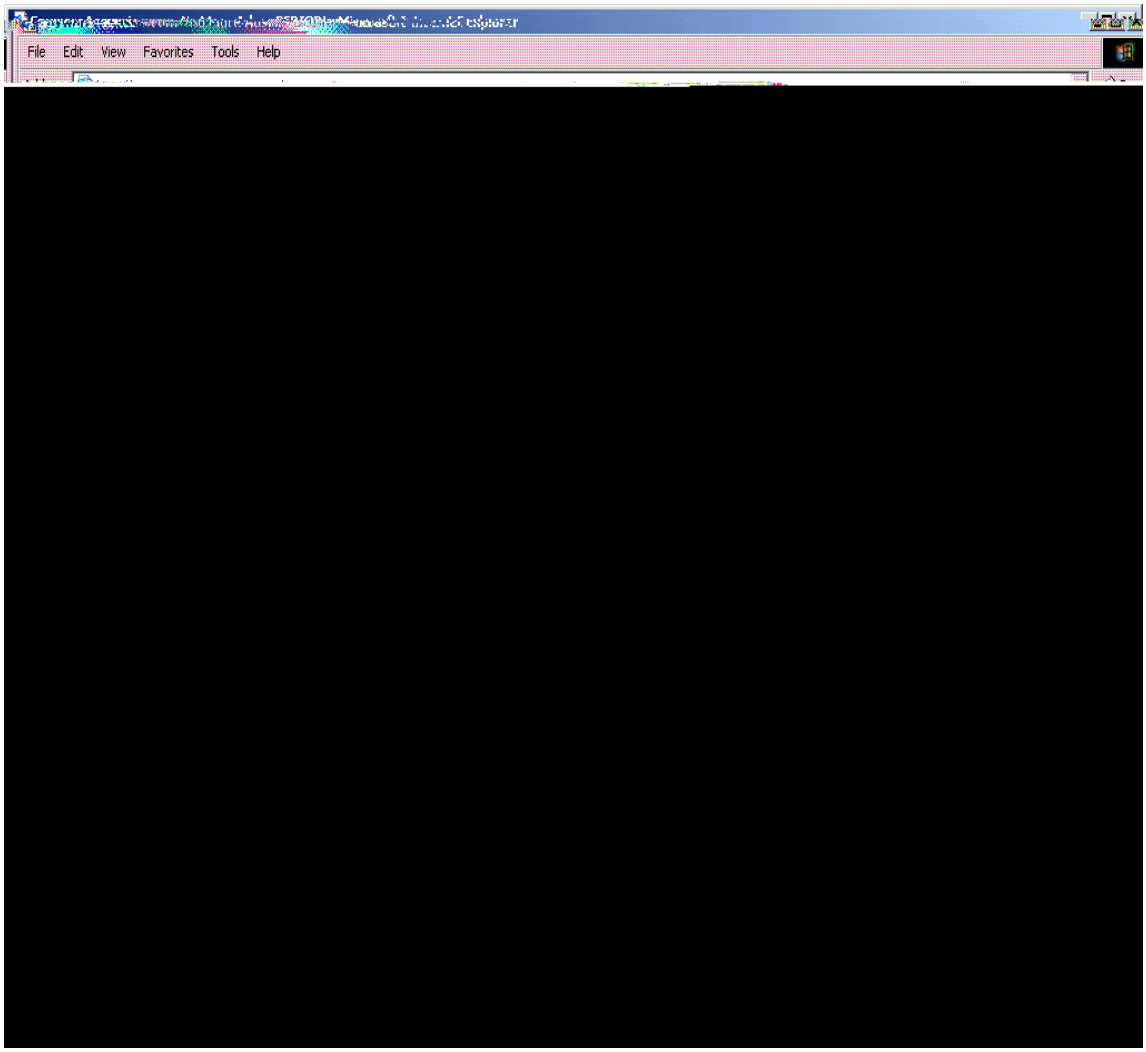
19. In numerous instances, the defendants' free locally-performed spyware scan is phony, and the defendants' representations that they have detected spyware on the consumer's computer are deceptive. In fact, in numerous instances, even when a scanned computer is "clean" prior to the defendants' scan and does not contain any spyware, the defendants represent that spyware has been detected. The file folders that the defendants claim contain the identified spyware are either

empty or contain innocuous files that do not contain the identified spyware or any other type of spyware.

Deceptive Spyware Removal Claims

20. In their marketing media, the defendants represent that they will remove all or substantially all of the spyware that has already been installed on a consumer's computer. For example, on their web site, www.spywareassassin.com, the defendants claim that they will "remove all spyware programs and files," "prevent any future breaches," "locate any and all spyware" and then provide a mechanism to remove it. Attached as Exhibit C below is a screen-shot of a portion of the defendants' web site:

Exhibit C



21. In numerous instances, the defendants do not remove "any and all," or even substantially all, of the spyware that is installed on a computer. Rather, in numerous instances, the defendants' "anti-spyware" software leaves intact significant amounts of spyware remaining on

that computer.

COUNT ONE

Deceptive Spyware Detection Claims

22. In numerous instances, in the course of marketing, selling, and

COUNT TWO

Deceptive Spyware Removal Claims

25. In numerous instances, in the course of marketing, selling, and distributing their "anti-spyware" software, the defendants have represented, expressly or by implication, that the defendants' "anti-spyware" software removes all, or substantially all, of the spyware that is currently installed on a consumer's computer.

26. In truth and in fact, in numerous instances, the defendants' "anti-

Court, the defendants are likely to continue to injure consumers and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

29. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and other ancillary relief, including consumer redress, disgorgement and restitution, to prevent and remedy any violations of any provision of law enforced by the Federal Trade Commission.

PRAYER FOR RELIEF

WHEREFORE, plaintiff, the Federal Trade Commission, requests that this Court, as authorized by Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and pursuant to its own equitable powers:

1. Award plaintiff such preliminary injunctive and ancillary relief as may be necessary to avert the likelihood of consumer injury during the pendency of this action and to preserve the possibility of effective final relief.

2. Permanently enjoin the defendants from violating Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), as alleged in this complaint.

3. Award such relief as the Court finds necessary to redress injury to consumers resulting from the defendants' violations of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), including, but not limited to, rescission of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies.

4. Award the Commission the costs of bringing this action, as well as any other equitable relief that the Court may determine to be just and proper.

Dated: March ___, 2005

Respectfully submitted:

WILLIAM BLUMENTHAL
General Counsel

_____

Mona Sedky Spivack, DC #447968
J. Ronald Brooke, Jr., MD #0202280002
Federal Trade Commission
600 Pennsylvania Ave., NW, Room 238
Washington, D.C. 20580
(202) 326-3795 (Spivack)
(202) 326-3484 (Brooke)
(202) 326-3395 FACSIMILE