

1 Mona Sedky Spivack, DC #447968
2 J. Ronald Brooke, Jr., MD #0202280002
3 Attorneys for Plaintiff Federal Trade Commission
4 600 Pennsylvania Ave., NW, Room 238
5 Washington, D.C. 20580
6 (202) 326-3795 (Spivack)
7 (202) 326-3484 (Brooke)
8 (202) 326-3395 FACSIMILE

9
10
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WASHINGTON

11 FEDERAL TRADE COMMISSION,

12
13 Plaintiff,

14 v.

15
16 MaxTheater, Inc., a Washington
17 corporation,

18
19 Thomas L. Delanoy, individually and
20 as an officer of MaxTheater, Inc.,

21 Defendants.
22
23
24
25
26

CIVIL NO.

Complaint for Injunctive
and Other Equitable Relief

1 Plaintiff, the Federal Trade Commission (“FTC” or “Commission”), for its
2 complaint alleges as follows:
3

- 4 1. The Commission brings this action under Section 13(b) of the Federal
5 Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), to obtain
6 preliminary and permanent injunctive relief against the defendants to
7 prevent them from engaging in deceptive acts or practices in violation
8 of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and to obtain other
9 equitable relief, including rescission, restitution, and disgorgement, as
10 is necessary to redress injury to consumers and the public interest
11 resulting from the defendants’ violations of the FTC Act.
12
13
14

15 **JURISDICTION AND VENUE**

- 16
17 2. Subject matter jurisdiction is conferred upon this Court by 15 U.S.C.
18 §§ 45(a), 53(b), and 28 U.S.C. §§ 1331, 1337(a), and 1345.
19
20 3. Venue in the United States District Court for the Eastern District of
21 Washington is proper under 15 U.S.C. § 53(b), as amended by the
22 FTC Act Amendments of 1994, Pub. L. No. 103-312, 108 Stat. 1691,
23 and 28 U.S.C. §§ 1391(b) and (c).
24
25
26

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

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).

17
18
19
20
21
22
23
24
25
26

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.

1 software products, including, but not limited to, “SpywareAssassin.”
2
3 The defendants market their purported “anti-spyware” software on
4 their web site and in text and html advertisements and messages
5 (including dialog boxes, windows, banners, buttons, icons, and/or
6 pop-ups and pop-unders) that appear on their web site, on the web
7 sites of their “affiliate” marketers, and on the computers that install
8 and operate the defendants’ “anti-spyware” software.
9

- 10 9. In an effort to induce consumers to purchase and download the
11 defendants’ “anti-spyware” software from their web site, the
12 defendants make numerous material deceptive representations in their
13 marketing media. First, after describing the various dangers of
14 spyware surreptitiously installed on a computer, the defendants
15 represent that they have “scanned” or otherwise examined the
16 consumer’s computer and have detected that spyware already resides
17 on it. In numerous instances, the defendants make these spyware
18 detection claims when the computer has no spyware residing on it.
19
20 Second, the defendants represent that their “anti-spyware” software,
21 which they sell for approximately \$29.95, removes all or substantially
22 all of the spyware that resides on a computer. In numerous instances,
23
24
25
26

1 the defendants make these spyware removal claims when the
2 defendants' "anti-spyware" software fails to remove significant
3 amounts of spyware that resides on a computer.
4

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

11 **Deceptive Spyware Detection Claims**

- 12
- 13 11. In their marketing media, the defendants define spyware, describe the
14 dangers associated with it, and then claim that they have scanned or
15 otherwise examined the consumer's computer and detected that the
16 consumer's computer already has spyware installed on it.
17
- 18 12. For example, on their web site, www.spywareassassin.com, the
19 defendants warn that "spyware & adware are harmful programs which
20 secretly install on your computer without your permission or
21 knowledge . . . decrease your computers [sic] performance [and cause]
22 the flood of popup ads . . . and is responsible for many harmful ads &
23 tactics, including: pop-ups, banner ads, highjacked search engine
24
25
26

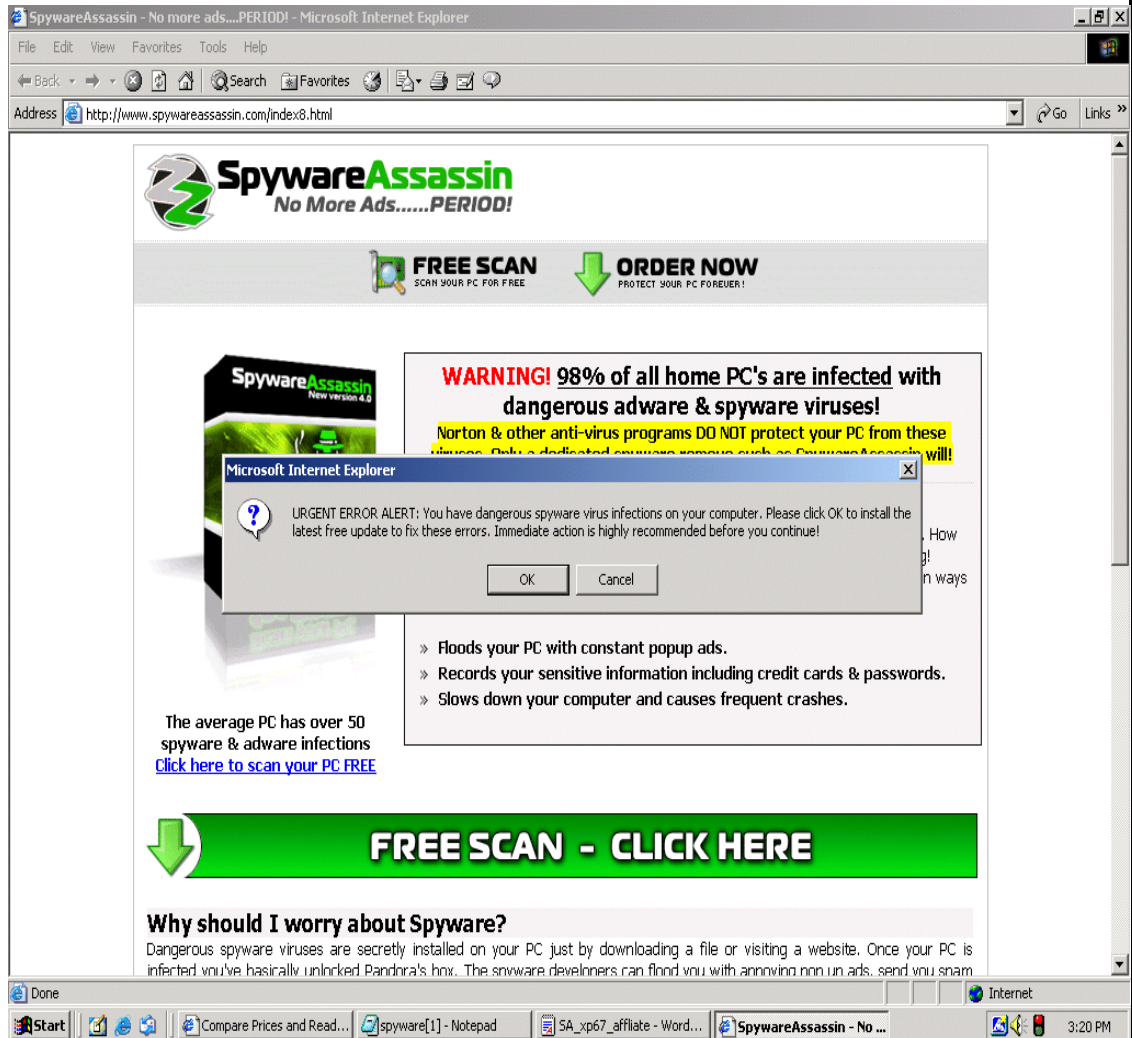
1 links, hijacked homepages, spam emails, activity tracking, file
2 stealing, credit card theft, fatal Trojan viruses, remote PC access, slow
3 internet connection [that will] ultimately . . . eventually damage your
4 computer so significantly that it will cease from working.” The
5 defendants unequivocally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

10
11
12
13 13. In their marketing media, the defendants also purport to perform two
14 types of free spyware scans on consumers’ computers. One scan is
15 purportedly performed remotely and is initiated automatically by the
16 defendants when a consumer visits or lands on certain portions of the
17 defendants’ web site. The other scan is purportedly performed locally
18 and is initiated by the consumer when the consumer installs and runs
19 the defendants’ software product. In either case, the defendants claim
20 that their scans have detected that the consumer’s computer already
21 has spyware installed on it.
22
23
24

25 14. With regard to the defendants’ remote spyware scan, the defendants
26

1 automatically display a spyware detection “pop up” message that
2 “pops up” on a consumer’s computer screen within seconds after a
3 consumer visits, or lands on certain pages of the defendants’ web site,
4 such as www.spywareassassin.com/index8.html. In their “pop up”
5 message, the defendants state in bold text: “URGENT ERROR
6 ALERT: You have dangerous spyware virus infections on your
7 computer. Please click OK to install the latest free update to fix these
8 errors. Immediate action is highly recommended before you
9 continue!” Attached as Exhibit A below is a screen-shot of the
10 defendants’ spyware detection “pop up” message:
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

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

1 know (and cannot know) whether the consumer’s computer in fact
2 already has “spyware” installed on it. At this point, the consumer’s
3 computer has not yet been scanned or otherwise examined for
4 spyware. The defendants display their spyware detection “pop up”
5 message automatically, regardless of whether the consumer has
6 clicked on the defendants’ “free scan”/download icons or otherwise
7 initiated the defendants’ local spyware scan described below. Further,
8 in numerous instances the defendants display their spyware detection
9 “pop up” even when, in fact, the computer is “clean” and does not
10 have spyware installed on it.
11

- 12
- 13
- 14 16. With regard to the defendants’ free local scan, the defendants state on
15 their web site that “Spyware Assassin . . . will scan your entire system
16 [for] all spyware programs . . .” and “will perform an initial scan,
17 which will locate any and all spyware currently residing on your
18 system . . .” They display in their marketing media several icons or
19 buttons that are labeled “free scan” and free “demo” or trial download.
20 After a consumer clicks on one of these icons or buttons, the
21 defendants then guide the consumer through a series of steps to
22 download and install the defendants’ “anti-spyware” software and to
23
24
25
26

1 then run the software to perform the purported spyware scan.

2 17. During and at the culmination of the defendants' free purported local
3 scan, the defendants repeatedly represent that they have detected
4 spyware on the consumer's computer. For example, while the
5 defendants' local scan is in progress, the defendants display a window
6 on the consumer's computer screen that purports to provide a real-
7 time summary of the results of the scan. These scan results include
8 the quantity and types of spyware detected on the consumer's
9 computer, as well as the location of the file folders (denominated
10 "category" and "value") that contain the detected spyware.
11

12 18. In numerous instances, the defendants have stated in their scan results
13 window that their scan has detected several well-known software
14 programs installed on a computer, including, but not limited to,
15 "Gator," "Bargain Buddy," "Xupiter," and "Flash Track." The
16 defendants have also identified the location of the purported spyware,
17 listing several file folder names next to each of the identified pieces of
18 spyware. Attached as Exhibit B below is a screen-shot of the
19 defendants' scanning window:
20
21
22
23
24
25
26

Exhibit B



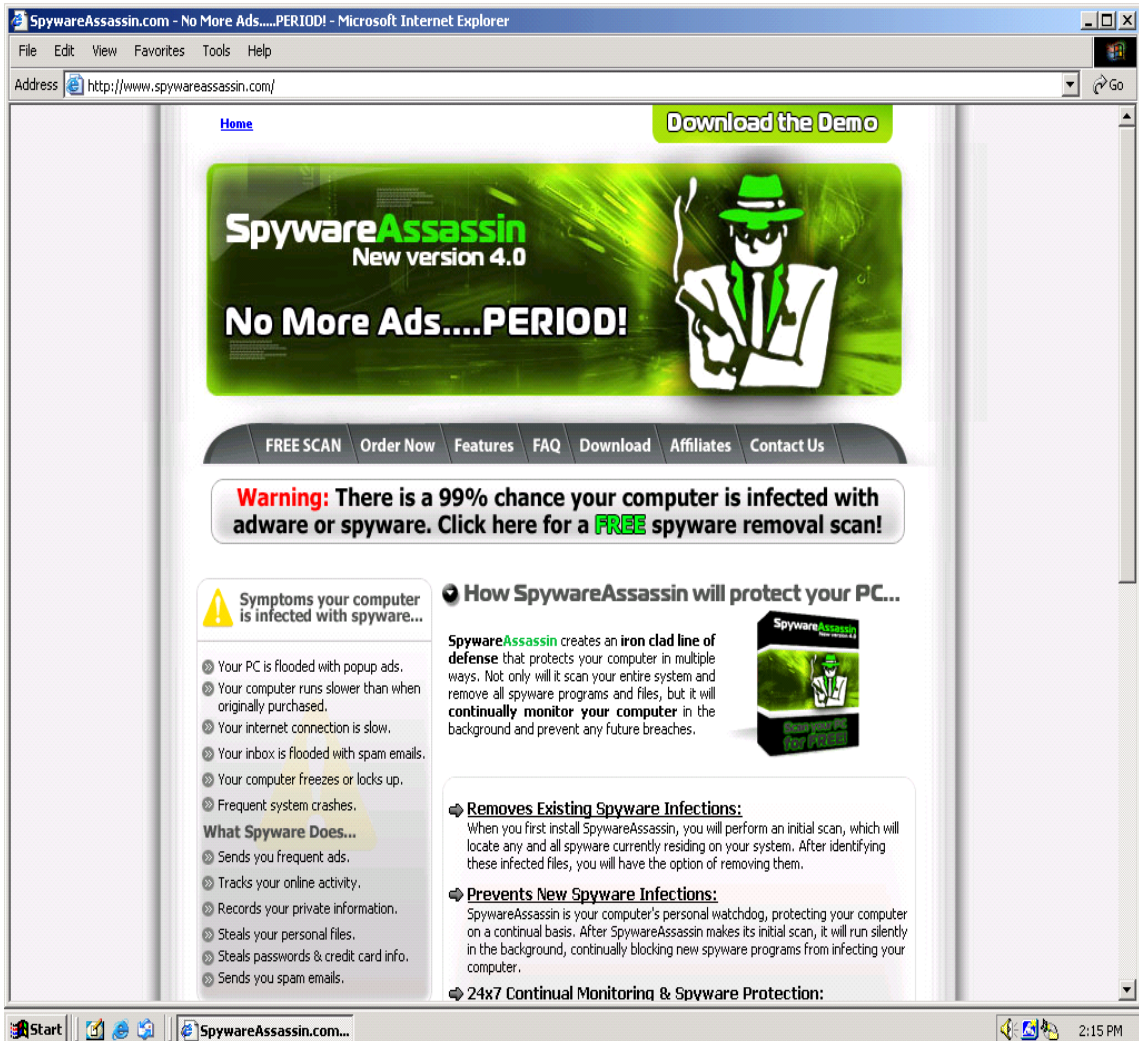
19. In numerous instances, the defendants’ free locally-performed spyware scan is phony, and the defendants’ representations that they have detected spyware on the consumer’s computer are deceptive. In fact, in numerous instances, even when a scanned computer is “clean” prior to the defendants’ scan 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

1 empty or contain innocuous files that do not contain the identified
2 spyware or any other type of spyware.
3

4 **Deceptive Spyware Removal Claims**

5
6 20. In their marketing media, the defendants represent that they will
7 remove all or substantially all of the spyware that has already been
8 installed on a consumer's computer. For example, on their web site,
9 www.spywareassassin.com, the defendants claim that they will
10 "remove all spyware programs and files," "prevent any future
11 breaches," "locate any and all spyware" and then provide a
12 mechanism to remove it. Attached as Exhibit C below is a screen-shot
13 of a portion of the defendants' web site:
14
15
16
17
18
19
20
21
22
23
24
25
26

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

1 that computer.

2 **COUNT ONE**

3 **Deceptive Spyware Detection Claims**

4
5 22. In numerous instances, in the course of marketing, selling, and
6 distributing their “anti-spyware” software, the defendants have
7 represented, expressly or by implication, that the defendants have,
8 either locally or remotely, scanned or otherwise examined the
9 consumer’s computer for spyware and have detected that the
10 consumer’s computer for spyware and have detected that the
11 consumer’s computer currently has spyware installed on it.

12
13 23. In truth and in fact, in numerous instances, the defendants have not
14 scanned or otherwise examined the consumer’s computer for spyware
15 and have not detected that the consumer’s computer currently has
16 spyware installed on it, as the defendants themselves have defined the
17 term.
18

19
20 24. Therefore, the defendants’ practices, as described in Paragraph 22
21 above, are deceptive and violate Section 5 of the FTC Act, 15 U.S.C.
22 § 45(a).
23
24
25
26

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

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-spyware” software does not remove all, or substantially all, of the spyware that is currently installed on a consumer’s computer, as the defendants themselves have defined the term.

27. Therefore, the defendants’ practices, as described in Paragraph 25 above, are deceptive and violate Section 5 of the FTC Act, 15 U.S.C. § 45(a).

22
23
24
25
26

CONSUMER INJURY

28. The defendants’ violations of Section 5 of the FTC Act, 15 U.S.C. § 45(a), as set forth above, have caused and continue to cause substantial injury to consumers. Absent injunctive relief by this

1 Court, the defendants are likely to continue to injure consumers and
2 harm the public interest.
3

4
5 **THIS COURT'S POWER TO GRANT RELIEF**

6 29. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court
7 to grant injunctive and other ancillary relief, including consumer
8 redress, disgorgement and restitution, to prevent and remedy any
9 violations of any provision of law enforced by the Federal Trade
10 Commission.
11
12

13 **PRAAYER FOR RELIEF**

14 WHEREFORE, plaintiff, the Federal Trade Commission, requests that this
15 Court, as authorized by Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and
16 pursuant to its own equitable powers:
17

- 18 1. Award plaintiff such preliminary injunctive and ancillary relief as
19 may be necessary to avert the likelihood of consumer injury during
20 the pendency of this action and to preserve the possibility of effective
21 final relief.
22
23 2. Permanently enjoin the defendants from violating Section 5(a) of the
24 FTC Act, 15 U.S.C. § 45(a), as alleged in this complaint.
25
26

