

RECEIVED

2000 MAR 25 AM 10:17

KING COUNTY  
SUPERIOR COURT CLERK  
SEATTLE, WA

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

**STATE OF WASHINGTON  
KING COUNTY SUPERIOR COURT**

STATE OF WASHINGTON,  
  
Plaintiff,  
  
v.  
  
RON COOKE, individually and as part  
of his marital community;  
  
MESSENGER SOLUTIONS, LLC, an  
Arizona limited liability company,  
  
Defendants.

NO. **08-2-10100-2 SEA**  
  
COMPLAINT FOR INJUNCTIVE  
AND ADDITIONAL RELIEF UNDER  
THE COMPUTER SPYWARE ACT,  
RCW 19.270, AND THE UNFAIR  
BUSINESS PRACTICES--  
CONSUMER PROTECTION ACT,  
RCW 19.86

COMES NOW PLAINTIFF, State of Washington, by and through its attorneys Robert  
M. McKenna, Attorney General and Katherine M. Tassi, Assistant Attorney General, and  
brings this action against Defendants named herein, alleging as follows on information and  
belief:

**I. JURISDICTION AND VENUE**

1.1 This Complaint is filed and these proceedings are instituted under the  
provisions of Chapter 19.270 RCW, the Computer Spyware Act; and Chapter 19.86 RCW, the  
Unfair Business Practices - Consumer Protection Act. Plaintiff seeks a permanent injunction  
and other equitable relief, including damages, restitution, civil penalties, and attorneys' costs and  
fees, based on violations of the Computer Spyware Act and the Unfair Business Practices -  
Consumer Protection Act.

COPY

1           1.2    The violations alleged in this Complaint have been and are being committed in  
2 whole or in part in King County, Washington, by Defendants named herein. Authority of the  
3 Attorney General to commence this action is conferred by RCW 19.86.080, RCW 19.86.140,  
4 and RCW 19.270.060.

## 5   **II.    DEFENDANTS**

6           2.1    Defendant Ron Cooke (“Cooke”), at all times relevant to this action, was  
7 directly engaged in the marketing and sale of software products over the Internet and by other  
8 means. Cooke resides at 6952 E. Hearn Rd., Scottsdale, Arizona 85254. Cooke is a Member  
9 of Messenger Solutions, LLC. Cooke is married to Jane Doe Cooke and together they  
10 constitute a marital community. All actions taken by Cooke as alleged in the Complaint herein  
11 are for the benefit of his marital community.

12           2.2    Defendant Messenger Solutions, LLC (“Messenger Solutions”), at all times  
13 relevant to this action, was directly engaged in the marketing and sale of software products  
14 over the Internet and by other means. Cooke, as a Member of Messenger Solutions, controls  
15 its policies, activities, and practices, including those alleged in the Complaint herein.  
16 Messenger Solutions’ principal place of business is at 6952 E. Hearn Rd., Scottsdale, Arizona  
17 85254

## 18   **III.    NATURE OF TRADE OR COMMERCE**

19           3.1    At all times material to this action, Cooke and Messenger Solutions (together,  
20 “Defendants”) have advertised, marketed, and offered for sale software products purportedly  
21 capable of preventing Windows Messenger Service pop-ups, also known as Net Send  
22 messages or Messenger Spam, from appearing on the consumer’s computer screen. The  
23 current name of the software product that Defendants are advertising and selling is Messenger  
24 Blocker. This program is sometimes marketed using different names. Defendants have also  
25 marketed and advertised products such as WinAntiVirus Pro 2007, a program purportedly  
26

1 capable of cleaning viruses from a consumer's computer, System Doctor and  
2 WinAntiSpyware. Defendants have marketed and/or sold these products to consumers all  
3 over the world via the Internet. Defendants transmit advertisements to a range of Internet  
4 Protocol (I.P.) addresses. Computers at those I.P. addresses that have Windows Messenger  
5 Service enabled will receive Defendants' pop-up advertisements. Windows Messenger  
6 Service is designed to provide computer network administrators with the ability to provide  
7 instant information to network computers, such as the need to log off the network due to a  
8 system malfunction. Because of its intended purpose, Messenger Service pop-up windows  
9 appear on a consumer's computer screen so long as the consumer is logged onto the network,  
10 i.e., connected to the Internet, no matter what application (e.g., word processing, spreadsheet,  
11 financial management) the consumer is using.

12           3.2 Defendants have co-opted this network administration utility by transmitting  
13 advertisements to consumers through Windows Messenger Service. By utilizing Messenger  
14 Service-type pop-ups, Defendants cause a large, grey-colored "window," or "dialogue box,"  
15 to appear near the middle of the consumer's computer screen. The "window" has a banner at  
16 the top that reads: "Messenger Service." The body of the "window" contains the text  
17 advertisement pitching Defendants' software that purports to block Windows Messenger  
18 Service pop-ups.

19           3.3 Prior to sending advertisements for his Messenger Service-blocking software to  
20 consumers' computer screens, Defendants bombard consumers' computers with a continuous  
21 stream of Messenger Service messages (i.e., pop-ups) advertising various products and  
22 services, including pornography and sexual-enhancement products. See Figures 1 and 2.  
23  
24  
25  
26

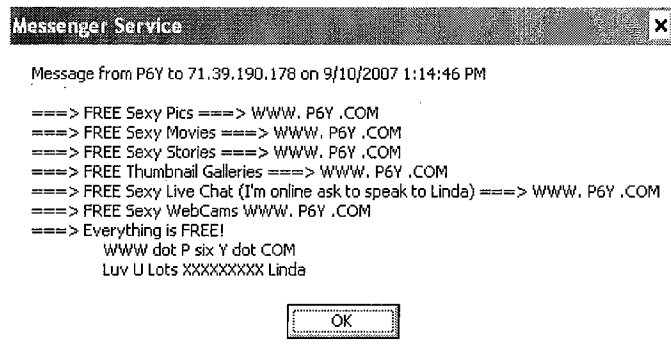


Figure 1.

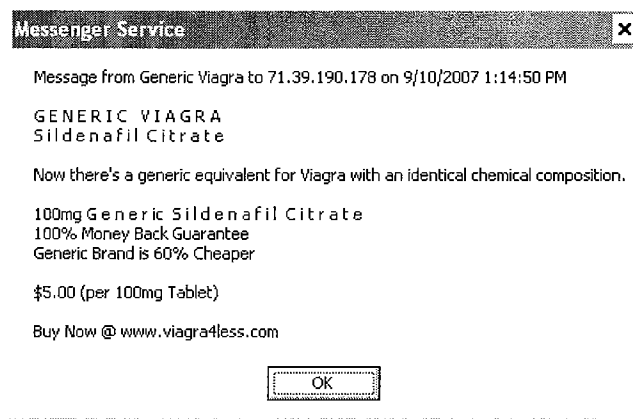
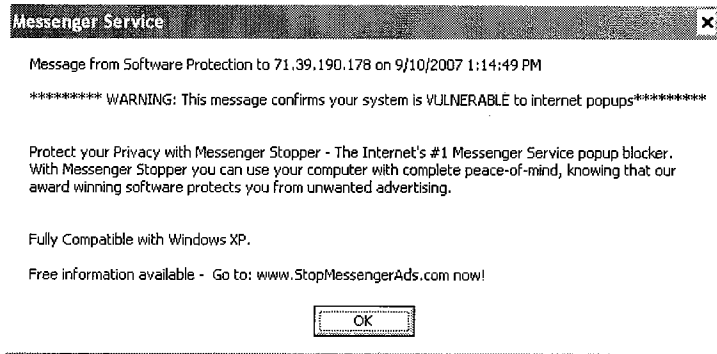
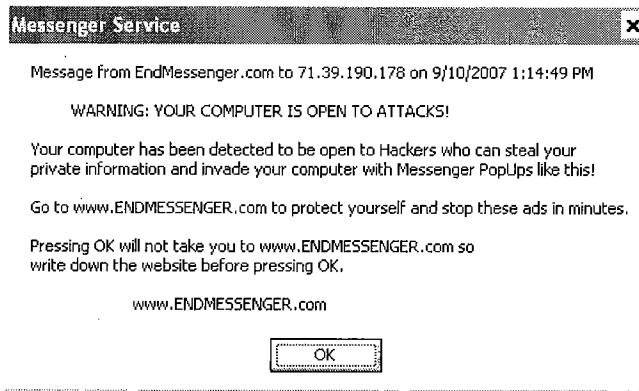


Figure 2.

3.4 However, these pop-ups are not advertisements for products or services that Defendants are actually offering for sale. Defendants then bombard the same consumers with alarmist Messenger Service messages claiming, among other things, that the consumers' computers are vulnerable to security attacks through Windows Messenger pop-ups. Defendants' advertisements also claim that the product will stop the very messages Defendants are sending. See Figures 3 and 4. The Messenger Service advertisements tell the consumer to go to a Web site that automatically re-directs to a Web site on which one of Defendants' products is sold.



8 Figure 3.



16 Figure 4.

17 3.5 In essence, Defendants attempt to coerce consumers into purchasing their pop-

18 up-blocking software by inundating consumers with pop-ups that will appear on their screens

19 no matter what they are doing, as long as they have an open connection to the Internet.

20 Sometimes they come so frequently as to cover the entire computer screen. A consumer's

21 only recourse might appear to be to turn their computer off.

22 3.6 Defendants have sold Messenger Blocker on various Web sites, including

23 www.messenger-blocker.com, www.endmessenger.com, and

24 www.blockmessengerspam.com. On some of Defendants' sites, they offer the software to the

25 consumer for a free 7-day trial period. On other sites, the product is available for purchase for

26 \$19.95 without a free trial period. Defendants' Web sites contain claims about the dangers of

1 Messenger Service advertisements, including that such messages are capable of “hacking” the  
2 consumer’s computer.

3           3.7     In order to get the free trial or to purchase the product, the consumer has to  
4 download software. Once downloaded and installed, the software behaves maliciously.  
5 Although it prevents Messenger Service messages from appearing on the consumer’s  
6 computer, it also causes the consumer’s computer to stealthily send out Messenger Service  
7 messages to other consumers’ computers that are identical to the ones that Defendants were  
8 sending to the consumer’s computer. These messages are transmitted at the approximate rate  
9 of one per every two seconds. The consumer does not even need to have a browser window  
10 open in order for their computer to be sending these Messenger Service advertisements. The  
11 computer only needs to be connected to the Internet.

12           3.8     During the trial period, the consumer’s computer does not receive Messenger  
13 Service messages. When the trial period of Messenger Blocker expires, the consumer’s  
14 computer is once again bombarded with what appear to be Messenger Service messages.  
15 However, in fact, they are messages generated by the software that Defendants have installed  
16 on the consumer’s computer. They are not real Messenger Service messages, but they appear  
17 even more frequently than the previous ones Defendants were transmitting, and they appear  
18 on the consumer’s computer whether or not the consumer is even connected to the Internet.  
19 These simulated Windows Messenger Service messages contain the same advertising text as  
20 Defendants’ messages transmitted through the Internet.

21           3.9     Furthermore, Defendants’ software is virtually impossible to uninstall. The  
22 program does not appear in the Add/Remove section of the consumer’s computer, nor is there  
23 an uninstall option offered to the consumer by any other means. In fact, even when various  
24 files related to the software are uninstalled, messages are still being sent from the computer.  
25  
26

1           3.10 Defendants' software disables Windows Task Manager in the user's computer.  
2 Task Manager is a Windows component that can be accessed by holding down Ctrl, Shift, and  
3 Esc at the same time. Task Manager provides detailed information about computer  
4 performance and running applications, processes and CPU usage, memory information,  
5 network activity and statistics, logged-in consumers, and system services. Task Manager can  
6 also be used to set process priorities, processor affinity, forcibly terminate processes, and shut  
7 down, restart, hibernate or log off from Windows. After Defendants' software is installed,  
8 when the consumer tries to access Task Manager, the message in Figure 5 appears.



9  
10  
11  
12  
13  
14 Figure 5.

15           3.11 In addition, Defendant's software changes the bookmarks on the computer by  
16 adding a bookmark for Defendants' Messenger Blocker Web site.

17           3.12 Defendants advertise, market, promote, and sell their products to consumers in  
18 Washington State and across the United States. Hundreds of consumers in Washington State  
19 have received Defendants' advertisements. Defendants are in competition with others  
20 engaged in the sale and marketing of these products in and from Washington.

21                           **VIOLATIONS OF THE COMPUTER SPYWARE ACT**

22                           **IV. First Cause of Action – Modifying Computer Settings**

23           4.1 Plaintiff realleges paragraphs 1.1 through 3.12 above and incorporates them as  
24 though fully set forth herein.

25           4.2 Defendants' Messenger Blocker software, both the trial and the registered  
26 versions, causes Defendants' Web site, [www.messenger-blocker.com](http://www.messenger-blocker.com), to be added to the

1 consumer's Internet bookmarks. Defendants' software modifies the settings on the computer  
2 that control the Internet browser's bookmarks. Defendants do not disclose either before,  
3 during, or after the installation process that the program will modify the consumer's list of  
4 bookmarks.

5 4.3 The conduct described above violates the Washington Computer Spyware Act,  
6 RCW 19.270.020(c), which prohibits modifying, through intentionally deceptive means,  
7 settings that control the owner or operator's list of bookmarks used to access web pages.  
8

9 **V. Second Cause of Action – Misrepresentation of the Necessity of Software for**  
10 **Security Purposes**

11 5.1 Plaintiff realleges paragraphs 1.1 through 4.3 above and incorporates them as  
12 though fully set forth herein.

13 5.2 Many of Defendants' Windows Messenger Service advertisements claim that  
14 the consumer's computer is vulnerable to "attacks" and "hackers" from Messenger Service  
15 advertisements and therefore needs Defendants' pop-up blocking software. In fact, the  
16 consumer's computer is not vulnerable to attacks or hackers from Messenger Service  
17 advertisements.

18 5.3 Defendants knowingly and intentionally misrepresent to consumers that the  
19 software they are promoting is necessary for security purposes in order to induce consumers to  
20 install the software; in fact, the software is not necessary at all.

21 5.4 The conduct of Defendants described above violates the Computer Spyware  
22 Act, RCW 19.270.040(1), which makes it unlawful for a person who is not an owner or operator  
23 of a consumer's computer to induce an owner or operator to install a computer software  
24 component onto the computer by intentionally misrepresenting the extent to which installing  
25 the software is necessary for security purposes.  
26





1 **VII. Fourth Cause of Action – Deceptively Causing User to Violate Computer Spyware**  
2 **Act**

3 7.1 Plaintiff realleges paragraphs 1.1 through 6.3 above and incorporates them as  
4 though fully set forth herein.

5 7.2 Defendants deceptively lure consumers into installing his Messenger Blocker,  
6 which, when executed, causes the user's computer, via Windows Messenger Service, to  
7 transmit to numerous other computers deceptive and misleading Messenger Service  
8 advertisements that intentionally misrepresent the necessity of the advertised product for  
9 security purposes whenever the user connects to the Internet.

10 7.3 The conduct of Defendants described above violates the Computer Spyware  
11 Act, RCW 19.270.040(2), which makes it unlawful for a person who is not an owner or operator  
12 of a consumer's computer to deceptively cause the execution of a software component with the  
13 intent of causing the user the use the component in a manner that violates any other provision  
14 of the Computer Spyware Act.  
15

16 **VIOLATIONS OF THE CONSUMER PROTECTION ACT**

17 **VIII. Fifth Cause of Action – Failure to Disclose Software's Functions**

18 8.1 Plaintiff realleges paragraphs 1.1 through 7.3 above and incorporates them as  
19 though fully set forth herein.

20 8.2 Defendants represent that their software is designed to block Messenger Service  
21 pop-ups. Defendants, however, fail to disclose numerous material facts about the software,  
22 including, but not limited to: a) the software has the ulterior purpose of causing the consumer's  
23 computer to transmit Messenger Service pop-up advertisements to remote I.P. addresses; b) the  
24 software contains code that will cause simulated Messenger Service pop-ups to appear on the  
25 consumer's computer as soon as the free trial period is over; c) the software adds a bookmark  
26

1 to the consumer's list of bookmarks; d) the software is difficult, if not impossible, to uninstall;  
2 and e) the software disables Windows Task Manager, making it impossible for the consumer to  
3 see what processes and applications are running on the computer.

4 8.3 The failure to disclose material facts such as those listed above constitutes  
5 unfair and deceptive acts or practices in trade or commerce and unfair methods of competition in  
6 violation of the Unfair Business Practices - Consumer Protection Act, RCW 19.86.020.

7 **IX. Sixth Cause of Action –Unfair and Deceptive Use of Consumers’ Computers**

8 9.1 Plaintiff realleges paragraphs 1.1 through 8.3 above and incorporates them as  
9 though fully set forth herein.

10 9.2 Defendants’ software, once installed on the user’s computer, causes the  
11 computer to transmit over the consumer’s Internet connection an unlimited number of  
12 Defendants’ Messenger Service advertisements unbeknownst to the consumer. Defendants’  
13 software causes the consumer’s computer to bombard other consumers’ computers with  
14 deceptive and misleading advertisements for Defendants’ products thereby perpetuating the  
15 cycle of infecting consumer’s computers with Defendants’ stealth software.

16 9.3 Making authorized, undisclosed, and stealth use of consumers’ computers and  
17 Internet connections constitutes unfair and deceptive acts or practices in trade or commerce and  
18 unfair methods of competition in violation of the Consumer Protection Act, RCW 19.86.020.

19 **X. Seventh Cause of Action – Unfair and Deceptive Interference with Computer**

20 10.1 Plaintiff realleges paragraphs 1.1 through 9.3 above and incorporates them as  
21 though fully set forth herein.

22 10.2 In many instances, Defendants interfere with consumers’ use of their computers  
23 by causing a stream of multiple, unwanted Windows Messenger Service pop-ups to appear on  
24  
25  
26

1 consumers' computer screens even when consumers are not using their Internet browsers.  
2 Moreover, if the consumer installs the free trial version of Messenger Blocker, as soon as the  
3 trial period has expired, Defendants' software causes a steady stream of advertisements for the  
4 software product to appear on the consumer's computer screen, even when the computer is not  
5 connected to the Internet. Consumers cannot proceed with their activity on the computer until  
6 they close each one of the advertisements individually. In at least one instance, over 3000  
7 advertisements were transmitted to a computer in a 24-hour period.  
8

9 10.3 The conduct described above constitutes unfair and deceptive acts or practices in  
10 trade or commerce and unfair methods of competition in violation of the Consumer Protection  
11 Act, RCW 19.86.020.

12 **XI. Eighth Cause of Action – Unfair and Deceptive Attempt to Coerce Consumers into**  
13 **Purchasing Software**

14 11.1 Plaintiff realleges paragraphs 1.1 through 10.3 above and incorporates them as  
15 though fully set forth herein.

16 11.2 In numerous instances, by causing at first a steady stream of unwanted  
17 Windows Messenger pop-ups advertising pornography and sexual-enhancement products and  
18 services to appear on the consumer's computer screen, followed by a steady stream of  
19 unwanted pop-ups advertising his products to stop pop-ups, Defendants attempt to coerce  
20 consumers into purchasing their software product to stop the stream of Messenger pop-ups that  
21 they have been transmitting.  
22

23 11.3 Furthermore, when a consumer agrees to a free trial of his software, and the  
24 consumer installs the software, Defendants' software causes yet another steady stream of  
25 unwanted Windows Messenger pop-ups to appear after the trial period expires on the  
26

1 consumer's computer screen even when the consumer is not connected to the Internet.  
2 Defendants attempt to coerce consumers into purchasing his software product to stop the  
3 stream of Messenger pop-ups that he has been causing.

4 11.4 The conduct described above constitutes unfair and deceptive acts or practices in  
5 trade or commerce and unfair methods of competition in violation of the Consumer Protection  
6 Act, RCW 19.86.020.

7  
8 **XII. Ninth Cause of Action – Unfair and Deceptive Stealth Installation of Software**

9 12.1 Plaintiff realleges paragraphs 1.1 through 11.4 above and incorporates them as  
10 though fully set forth herein.

11 12.2 Defendants' software installs itself in remote, unidentifiable locations, making it  
12 impossible for consumers to locate its files and/or uninstall it. Defendants' software does not  
13 appear in the Add/Remove section of Windows Control Panel. Defendants do not provide  
14 consumers with an uninstall option for his software. If the consumer does not purchase  
15 Defendants' product, the consumer will continue to be subjected to the pop-up advertisements  
16 generated by their trial software because the consumer cannot locate the software files to  
17 uninstall them. In addition, the user's computer will continue to send Messenger Service  
18 advertisements to other consumers' computers.

19  
20 12.3 The conduct described above constitutes unfair and deceptive acts or practices in  
21 trade or commerce and unfair methods of competition in violation of the Consumer Protection  
22 Act, RCW 19.86.020.  
23  
24  
25  
26

1 **XIII. Tenth Cause of Action – Unfair and Deceptive Transmission of Malicious Software**

2 13.1 Plaintiff realleges paragraphs 1.1 through 12.3 above and incorporates them as  
3 though fully set forth herein.

4 13.2 Defendants, without the consent, authorization, or knowledge of the consumer,  
5 cause to be transmitted, downloaded, and installed on the user's computer malicious software  
6 that turns the consumer's computer into a Messenger Service spamming machine, which in  
7 turn infects potentially hundreds to thousands of other consumers' computers.  
8

9 13.3 Surreptitiously transmitting malicious software and causing it to be installed on  
10 the user's computer constitutes unfair and deceptive acts or practices in trade or commerce and  
11 unfair methods of competition in violation of the Consumer Protection Act, RCW 19.86.020.  
12

13 **XIV. PRAYER FOR RELIEF**

14 WHEREFORE, Plaintiff, State of Washington, prays for relief as follows:

15 14.1 That the Court adjudge and decree that Defendants have engaged in the  
16 conduct complained of herein.

17 14.2 That the Court adjudge and decree that the conduct complained of in  
18 paragraphs 4.1 through 7.3 constitutes violations of the Computer Spyware Act, RCW 19.270,  
19 *et seq.*

20 14.3 That the Court adjudge and decree that the conduct complained of in paragraphs  
21 8.1 through 13.3 constitutes unfair or deceptive acts and practices and unfair methods of  
22 competition in violation of the Consumer Protection Act, Chapter 19.86 RCW.

23 14.4 That the Court issue a permanent injunction enjoining and restraining  
24 Defendants, and their representatives, successors and assigns, officers, agents, servants,  
25 employees and all other persons acting or claiming to act for, or on behalf of, or in active  
26

1 concert or participation with Defendants, from continuing or engaging in unlawful conduct  
2 complained of herein.

3 14.5 That the Court assess a civil penalty, pursuant to RCW 19.86.140, of up to  
4 \$2,000 per violation against the Defendants for each violation of RCW 19.86.020 caused by  
5 the conduct complained of herein.

6 14.6 That the Court make such orders pursuant to RCW 19.86.020 as it deems  
7 appropriate to provide for restitution to consumers for money or property acquired by  
8 Defendants as a result of the conduct complained of herein.

9 14.7 That the Court make such orders pursuant to RCW 19.270.060 as it deems  
10 appropriate to provide recovery for damages for each violation of RCW 19.270.

11 14.8 That the Court make such orders pursuant to RCW 19.86.020 and RCW  
12 19.270.060 to provide that Plaintiff, State of Washington, have and recover from Defendants  
13 the costs of this action, including reasonable attorneys' fees.

14 14.9 That the Court order such other relief as it may deem just and proper to fully  
15 and effectively dissipate the effects of the conduct complained of herein, or which may  
16 otherwise seem proper to the Court.

17 DATED this 17<sup>th</sup> day of March, 2008.

18 ROBERT M. MCKENNA  
19 Attorney General

20  
21 

22 KATHERINE M. TASSI, WSBA #32908  
23 Assistant Attorney General  
24 Attorneys for Plaintiff  
25 State of Washington  
26