Sealed
Public and unofficial staff access
to this instrument are
prohibited by court order.



UNITED STATES COURTS SOUTHERN DISTRICT OF TEXAS FILED

MAY 3 1 2005

Michael N. Milby, Clerk of Court

UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF TEXAS

Civ. No.

05 1905

| | — <u> </u> | |
|--|------------|--|
| FEDERAL TRADE COMMISSION, |) | |
| Plaintiff, |) | |
| vs. |) | |
| TRUSTSOFT, INC. d/b/a |) | |
| SWANKSOFT and SPYKILLER, |) | |
| DANILO LADENDORF, individually and as an officer of Trustsoft, Inc., | | |
| Defendants |) | |
| |) | |

COMPLAINT FOR INJUNCTIVE AND OTHER EQUITABLE RELIEF

Plaintiff, the Federal Trade Commission ("FTC" or "Commission"), for its complaint alleges as follows:

1. The Commission brings this action under Sections 13(b) and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 53(b) and 57b, and the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act"), 15 U.S.C. §§ 7701 *et seq.*, to obtain preliminary and permanent injunctive relief, including rescission, restitution, redress, disgorgement, and other equitable relief for defendants' deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, and the CAN-SPAM Act.

JURISDICTION AND VENUE

- 2. Subject matter jurisdiction is conferred upon this Court by 15 U.S.C. §§ 45(a), 53(b), and 28 U.S.C. §§ 1331, 1337(a), and 1345.
- 3. Venue in this District is proper under 15 U.S.C. § 53(b) and 28 U.S.C. §§ 1391(b) and (c).

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 is charged, inter alia, with enforcement of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The Commission is also charged with enforcing various provisions of the CAN-SPAM Act as if a violation of the CAN-SPAM Act "were an unfair or deceptive act or practice proscribed under section 18(a)(1)(B) of the [FTC Act] (15 U.S.C. § 57a(a)(1)(B))." 15 U.S.C. § 7706(a). The Commission is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and the CAN-SPAM Act and to secure such equitable relief as may be appropriate.

DEFENDANTS

5. Defendant Trustsoft, Inc. ("Trustsoft"), formerly Swanksoft Technologies, Inc., is a Texas corporation with its purported principal place of business located at 1330 Post Oak Blvd., Suite 2300, Houston, Texas. At all times material to this complaint, Defendant Trustsoft does or has done business as "Swanksoft," "SpyKiller" and "SpyKiller.com." Defendant Trustsoft transacts or has transacted business in this District.

6. Defendant Danilo Ladendorf is president and owner of Defendant Trustsoft. At all times material to this complaint, Defendant Ladendorf, individually or in concert with others, has formulated, directed, controlled, or participated in the acts and practices of Defendant Trustsoft, including the acts and practices set forth in this complaint. Defendant Ladendorf does or has done business as "Swanksoft," "SpyKiller" and "SpyKiller.com." Defendant Ladendorf resides in and transacts or has transacted business in this District.

COMMERCE

7. At all times relevant to this complaint, defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANTS' BUSINESS PRACTICES

Overview

- 8. Since at least July 2003, defendants have marketed, sold, and distributed via the Internet "spyware" removal computer software products, including, but not limited to, SpyKiller 2003, SpyKiller 2004, and SpyKiller 2005 (collectively "SpyKiller"). Spykiller purports to scan a consumer's computer, identify all of the spyware residing on it, and then remove such spyware after consumers purchase and download the product from defendants' web sites.
- 9. Spyware poses a real danger to consumers' computers. The term "spyware" includes software programs surreptiously downloaded on a consumer's computer without the consumer's knowledge that can, among other things, track consumers' online activities, monitor their keystrokes, capture their personal information and passwords, change their established internet browser preferences, and bombard them with pop-up advertisements (such pop-up software and other advertising programs

are often referred to as "adware"). In addition, individually and collectively, such spyware programs can greatly impede the processing speed and performance of a consumer's computer, in some cases rendering the computer inoperable.

- 10. Defendants capitalize on consumers' legitimate fear of spyware by inducing consumers to download and purchase SpyKiller from defendants' web sites through deceptive marketing. Defendants aggressively and deceptively market their spyware removal software though a variety of marketing media, including on their web sites and the web sites of their "affiliate" marketers, in text and html advertisements and messages (including windows, banners, buttons, and/or pop-ups and pop-unders), and in commercial email messages (commonly referred to as "spam").
 - 11. Defendants' marketing media contain numerous material deceptive representations.
- 12. First, defendants represent, in pop-ups, banner ads, commercial email and other marketing media, that they have remotely "scanned" or otherwise examined a consumer's computer and have "detected" that spyware resides on it. In numerous instances, defendants make these remote scan and detection representations even when no scan or examination has taken place.
- 13. Second, after a consumer downloads SpyKiller from defendants' web page and activates the program's scanning capabilities, defendants make additional false assertions about the detection of spyware on the consumer's computer. Defendants make these detection misrepresentations both during the course of the SpyKiller scan and at the completion of the SpyKiller scan.
- 14. Third, defendants represent that their spyware removal software, which they sell for approximately \$39.95, removes all or substantially all of the spyware that resides on a computer, including specified spyware programs listed on defendants' web sites. In numerous instances when

defendants make these spyware removal claims, defendants' software fails to remove significant amounts of spyware that resides on a computer, including numerous specific spyware programs that defendants promise to remove.

- 15. Fourth, in numerous instances, defendants initiate commercial email messages ("spam") promoting SpyKiller that relate to purported spyware detections on a consumer's computer. Defendants fail to advise the consumer that such email messages are advertisements. In numerous instances, defendants' commercial email messages also contain false "from" line information and no valid postal address, thereby preventing consumers from identifying who transmitted the emails and from responding to the emails. Defendants' commercial email messages also fail in numerous instances to provide consumers with the required notice and ability to "opt-out" from similar commercial emails in the future.
- 16. Ultimately, in the course of marketing, selling, and distributing their spyware removal software, defendants make material false and misleading representations in their marketing media, and thereby engage in deceptive acts or practices in violation of Section 5 of the FTC Act. In addition, the commercial email initiated by defendants violates the CAN-SPAM Act.

Defendants' Deceptive Spyware Detection Claims

- 17. Defendants market SpyKiller by making numerous false representations in order to induce consumers to download and purchase SpyKiller.
- 18. Defendants market SpyKiller directly to consumers, principally through their web sites, including www.spykiller.com, www.trustsoft.com, and www.swanksoft.com, as well as paid search engine links to those web sites. Defendants also aggressively market SpyKiller through an extensive network of "affiliate" marketers, who promote SpyKiller to consumers through other web sites,

commercial e-mail messages, pop-ups, banner advertisements, and other electronic media that link to www.spykiller.com. Defendants' affiliates earn commissions on each sale of SpyKiller that they generate.

19. Defendants solicit affiliates via their affiliate program web site, www.killercash.com. In this regard, defendants have established hyperlinks to www.killercash.com from www.spykiller.com, www.trustsoft.com, and www.swanksoft.com. Defendants tout their "Killercash" affiliate program as one of the "Internet's top affiliate programs" with payouts to affiliates on each sale of SpyKiller of "up to 50%."



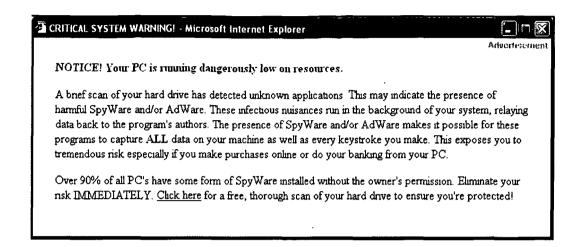
FTC Complaint Exhibit 1

Defendants' Deceptive Remote Scan Detection Claims

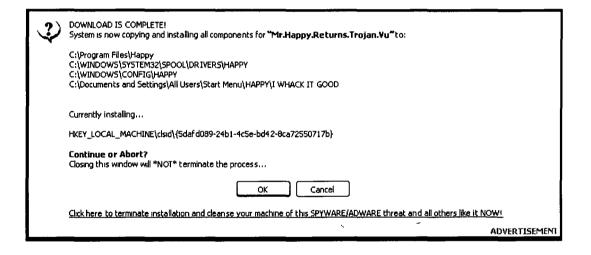
- 20. On their www.killercash.com web site, defendants provide their affiliates with sample marketing media, such as banner and pop-up advertisements, to use in marketing SpyKiller to consumers. In numerous instances, defendants make deceptive claims through these marketing media.
- 21. These "SpyKiller Advertisements" include deceptive banners and pop-ups that falsely inform consumers that a remote scan or examination has been performed on their computer and that spyware has been detected on their computers. These advertisements, which in numerous instances appear in the form of a warning purportedly generated by a computer's operating system, include the following:



FTC Complaint Exhibit 2



FTC Complaint Exhibit 3



FTC Complaint Exhibit 4

22. These deceptive advertisements are nothing more than computer graphics that have no computer scanning capabilities. Thus, the representations in these advertisements that scans or examinations have been performed and that spyware has been "detected" are inherently false. The deception of Exhibit 4 is particularly frightening for consumers, because the pop-up is constructed to scroll text at a rapid rate after the phrase "currently installing" This scrolling text gives consumers

the false impression that dangerous "trojan" programs are rapidly installing on their machines at that very moment.

- 23. In numerous instances, defendants also initiate deceptive commercial email premised on phony remote scans and detections.
- 24. Defendants' commercial email includes false messages concerning remote detections of spyware with the email subject header "Warning. Important Message!" The body of one such message states:

Warning. Important Message!

You are seeing this message, because the account

has been detected as having tracking software attached to it. (more info)

This is not a virus, but a program in your machine that **monitors** and transmits all of you online activities, and is a serious violation of your privacy.

Below is a link to a free scanner to <u>download</u> that will find and remove all spyware programs on your machine: <u>Get the scanner</u>

FTC Complaint Exhibit 5

- 25. In fact, in numerous instances, defendants initiate such email even though no remote scan or examination has taken place to determine if a consumer's computer has such "tracking" spyware that "monitors and transmits all of [the consumer's] online activities."
- 26. A consumer who wants to determine the SpyKiller purchase price from the defendants' web sites is faced with further remote detection misrepresentations. In this regard, a consumer who links

to the www.spykiller.com purchase page from www.trustsoft.com or www. swanksoft.com is presented (sometimes after a pause) with a purchase page that is headed in bold red lettering with the statement:

ALERT: You have Spyware and Adware parasite(s) on your computer right now!

WARNING: You need to unlock SpyKiller below to clean your system of Spyware now!

Unlock SpyKiller now and clean your system of Spyware AdWare and Keyloggers before it is TOO LATE!

This message has also appeared when linking to the purchase page directly from www.spykiller.com.

- 27. Contrary to this message, however, no spyware scan or examination of a consumer's computer occurs when landing on this purchase page. Rather, this deceptive statement appears regardless of whether there is any spyware on a consumer's computer, and thus even when there is no spyware present on a consumer's computer.
- 28. Therefore, in numerous instances, defendants' claims in their marketing media that a remote scan or examination has been performed on a consumer's computer are false, and defendants' representations that they have detected spyware on the consumer's computer are deceptive.

Defendants' Deceptive Post-Download Detection Claims

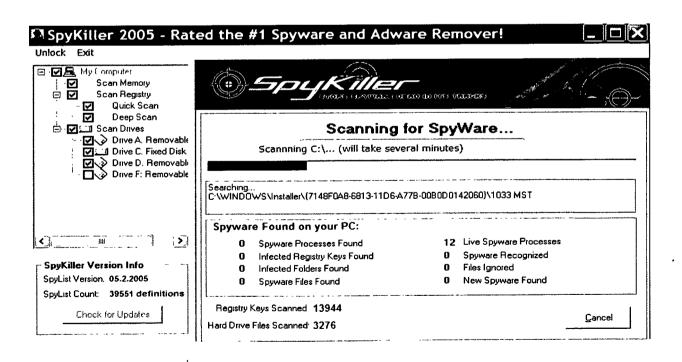
- 29. Consumers who succumb to defendants' phony remote scan and detection claims noted above, and therefore seek to learn more about defendants' spyware removal product, can connect by hyperlink from defendants' deceptive marketing media to defendants' www.spykiller.com web site.

 Consumers can download and purchase SpyKiller from this site.
- 30. Defendants offer on their www.spykiller.com web site to perform a "local" spyware scan of a consumer's computer for free. In order for SpyKiller to perform this local scan, a consumer must

first download SpyKiller. Only the download and local scan are free. Consumers who want to use SpyKiller to remove any spyware purportedly detected by the free scan must first purchase Spykiller from the purchase page of the web site. Once they have purchased SpyKiller, consumers are sent an "unlock code" by email that they can use to activate the spyware removal capabilities of SpyKiller.

- 31. Defendants make further material misrepresentations to consumers who download SpyKiller for the free scan.
- 32. For example, while the SpyKiller scan is running (the scan typically takes more than forty minutes to run) the program displays a status report that is entitled "Spyware Found on your PC:."

 Under this title is the category "Live Spyware Processes," which purports to report a numerical count of such "Live Spyware Processes" on the consumer's computer.



FTC Complaint Exhibit 6

- 33. In fact, the programs accounted for in the category "Live Spyware Processes" are <u>any</u> processes running on the computer at the time of the scan. For example, any anti-virus program, word processing program, or operating system program running on the computer constitutes a live process. Thus, in numerous instances, the SpyKiller scan informs consumers that "Live Spyware Processes" have been "Found" on their computers when no such spyware programs exist. The effect of defendants' representation is to induce consumers to purchase and activate the removal component of SpyKiller even before the lengthy system scan has been completed.
- 34. After the local SpyKiller scan is complete, SpyKiller displays a "detection report" listing the names of spyware that Spykiller has purportedly found on the consumer's computer. Next to the name of each spyware program purportedly detected, SpyKiller lists an assigned "danger level." However, SpyKiller is programed so that the only "level" assigned to each reported spyware program detected by SpyKiller is "SEVERE."
- 35. In numerous instances, SpyKiller detection reports include false positives that are triggered by harmless applications on consumers' computers that are not spyware. In other words, the scanning mechanism falsely identifies files from such applications as being spyware. These false positives mislead consumers to believe that their computers contain particularly insidious spyware programs.
- 36. For example, in numerous instances, SpyKiller generates a false detection report for the spyware Keycorder when consumers who have America Online ("AOL") on their computers run the SpyKiller scan. In fact, the file flagged by SpyKiller is a necessary and innocuous component of AOL. Keycorder, on the other hand, is a dangerous program that defendants' own www.trustsoft.com web site

describes as a "Key Logger" program "that records user keystrokes" and thus could be used to steal consumer passwords, credit card numbers, or other sensitive personal data.

Defendants' Deceptive Spyware Removal Claims

- 37. In their marketing media, defendants represent that SpyKiller will remove all or substantially all of the spyware that is on a consumer's computer. For example, on their www.swanksoft.com web site, defendants state that SpyKiller will "search and destroy all hidden Spyware, Adware, Keyloggers, Browser Hijackers and Malware programs on your computer." Similarly, on their www.spykiller.com web site, defendants state that SpyKiller "will remove the Spyware, Adware, Keyloggers, Browser Hijackers and Malware on your computer."
- 38. On defendants' www.trustsoft.com web site, defendants claim to remove "all traces" of thousands of described spyware programs. In this regard, defendants' web site includes a "spyware encyclopedia" that lists thousands of spyware programs, each of which defendants represent "SpyKiller is able to detect . . . and successfully remove all traces of as follows:

THREATS

Peper

» go to Spyware Threats home ...

» Threat updated at 17:34 on 04.06.2005

summary

The spyware threat, "Peper," has been categorized to the following types of threat(s): Trojan, Trojan Tool.

» Trojan:

• Trojan (a.k.a. trojan horse) is a malicious program that is disguised as legitimate software. A Trojan horse can be deliberately attached to otherwise useful software by a programmer, or it can be spread by tricking users into believing that it is a useful program. Trojan horses can be designed to do various harmful things such as erasing or overwriting data on a computer, corrupting files in a subtle way spreading other malware, such as viruses, setting up networks of zombie computers in order to launch DDoS attacks or send spam, spying on the user of a computer and covertly reporting data like browsing habits to other people, phish for bank or other account details, which can be used for criminal activities. or installing a backdoor on a computer system.

» Trojan Tool:

A tool that is utilized by a malicious Trojan for a variety of purpouses.
 These tools may help spread the Trojan or help by disabling security features on the host machine.

removal

- SpyKiller is able to detect this threat
- SpyKiller successfully removes all traces of this threat

Click here for a FREE SpyKiller System Scan!

5/4/2005 3:05:56 PM

FTC Complaint Exhibit 7

- 39. Various other of defendants' marketing media, including their pop-ups and email, also claim that SpyKiller will "eliminate" or remove "all" of the spyware present on a computer.
- 40. However, in numerous instances, defendants do not remove "all," or even substantially all, of the spyware that is installed on a computer. Rather, in numerous instances, SpyKiller does not remove

significant amounts of spyware on a computer, including specific spyware programs it promises to remove.

Defendants' Unlawful Commercial Email

- 41. Defendants initiate commercial email promoting SpyKiller. As noted above, such email messages include false representations that spyware has been detected on the computers of consumers receiving these messages. Such commercial email messages also fail to identify that they are advertisements.
- 42. In addition, defendants initiate commercial email messages that contain false "header" information, including email that display a phony "from" email address line or that display no "from" line information at all. These false headers create consumer uncertainty about who sent the email messages. In this regard, in numerous instances where recipients configure their email software to reveal maximal "from" information about an email message, defendants give recipient consumers the false impression that the SpyKiller email was sent by the recipient consumer's internet service provider ("ISP").
- 43. Defendants also initiate commercial email messages that fail to include a valid postal address. As a result, consumers may have difficulty determining who sent such messages.
- 44. In numerous instances, defendants also initiate commercial email messages that fail to notify recipients of their ability to decline receiving future email messages from defendants (an "optout"), and that fail to include a reply email address or other mechanism that recipients can use to decline receiving future email messages from defendants. As a result, consumers cannot reply to such messages or communicate their right to "opt-out" from receiving future commercial email messages from a sender.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

45. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "deceptive" acts and practices in or affecting commerce. Misrepresentations or omissions of material fact constitute "deceptive" acts or practices pursuant to Section 5(a) of the FTC Act.

COUNT ONE

Defendants' Deceptive Remote Scan Spyware Detection Claims

- 46. In numerous instances, in the course of marketing, selling, and distributing their spyware removal software, defendants represent or have represented, expressly or by implication, that they remotely scan or otherwise examine a consumer's computer for spyware and detect that the consumer's computer has spyware installed on it.
- 47. In truth and in fact, in numerous instances, defendants do not remotely scan or otherwise remotely examine the consumer's computer for spyware and do not remotely detect that the consumer's computer has "spyware" installed on it, as the defendants define that term.
- 48. Therefore, defendants' practices as described in Paragraph 46 are deceptive and violate Section 5 of the FTC Act, 15 U.S.C. § 45(a).

COUNT TWO

Defendants' Deceptive Post-Download Spyware Detection Claims

49. In numerous instances, in the course of marketing, selling, and distributing their spyware removal software, and after a consumer downloads and activates the defendants' local scan for spyware, defendants represent or have represented, expressly or by implication, that certain software or applications on the consumer's computer are spyware.

- 50. In truth and in fact, in numerous instances, such software or applications are not "spyware" as the defendants' define that term.
- 51. Therefore, defendants' practices as described in Paragraph 49 are deceptive and violate Section 5 of the FTC Act, 15 U.S.C. § 45(a).

COUNT THREE

Defendants' Deceptive Spyware Removal Claims

- 52. In numerous instances, in the course of marketing, selling, and distributing their spyware removal software, defendants represent or have represented, expressly or by implication, that defendants' spyware removal software removes all, or substantially all, of the spyware that is installed on a consumer's computer, including, but not limited to, "all traces" of particular spyware programs listed on defendants' web sites.
- 53. In truth and in fact, in numerous instances, defendants' spyware removal software does not remove all, or substantially all, of the spyware that is installed on a consumer's computer, including, but not limited to, "all traces" of particular spyware programs listed on defendants' web sites.
- 54. Therefore, defendants' practices as described in Paragraph 52 are deceptive and violate Section 5 of the FTC Act, 15 U.S.C. § 45(a).

VIOLATIONS OF THE CAN-SPAM ACT

55. The CAN-SPAM Act, 15 U.S.C. §§ 7701 et seq. (2004), became effective on January 1, 2004. The CAN-SPAM Act makes it unlawful to initiate commercial email that *inter alia*: contains materially false or misleading header information, does not contain a clear and conspicuous identification that the message is an advertisement or solicitation, does not contain a clear and conspicuous notice of

the opportunity to decline to receive further commercial electronic mail messages from the sender, does not contain a functioning return electronic mail address or another opt-out mechanism, or does not contain a valid physical postal address of the sender.

COUNT FOUR

Defendants' CAN-SPAM Act Violations

- 56. In numerous instances, Defendants have initiated the transmission, to protected computers, of commercial email messages that:
- A. contain or are accompanied by materially false or materially misleading header information;
- B. do not include clear and conspicuous notice of the recipient's opportunity to decline to receive further commercial electronic mail messages from the sender at the recipient's electronic mail address;
- C. do not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that a recipient could use to submit a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from the sender at the recipient's electronic mail address;
- D. do not include clear and conspicuous identification that the message is an advertisement or solicitation; or
 - E. do not include the sender's valid physical postal address.

57. Therefore, defendants' acts or practices as described above violate Sections 5(a)(1), 5(a)(5)(A)(i-iii), and/or 5(a)(3), of the CAN-SPAM Act, 15 U.S.C. §§ 7704(a)(1), § 7704(a)(5)(A)(i-iii), and/or § 7704(a)(3).

CONSUMER INJURY

58. Defendants' violations of Section 5 of the FTC Act, 15 U.S.C. § 45(a), and the CAN-SPAM Act, 15 U.S.C. §§ 7701 *et seq.*, as set forth above, have caused and continue to cause substantial injury to consumers. In addition, defendants have been unjustly enriched as a result of their unlawful practices. Absent injunctive relief by this Court, defendants are likely to continue to injure consumers and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

59. Sections 13(b) and 19 of the FTC Act, 15 U.S.C. §§ 53(b) and 57b, empower this Court to grant injunctive and other ancillary equitable relief, including consumer redress, disgorgement and restitution, to prevent and remedy any violations of any provision of law enforced by the Federal Trade Commission. A violation of the CAN-SPAM Act may be remedied in the same manner as a violation of the FTC Act. 15 U.S.C. § 7706(a) and (d).

PRAYER FOR RELIEF

WHEREFORE, plaintiff, the Federal Trade Commission, requests that this Court, as authorized by Sections 13(b) and 19 of the FTC Act, 15 U.S.C. §§ 53(b) and 57b, Section 7 of the CAN-SPAM Act, 15 U.S.C. § 7706, and pursuant to its own equitable powers:

- 60. 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.
- 61. Permanently enjoin defendants from violating Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), as alleged in this complaint.
- 62. Award such relief as the Court finds necessary to redress injury to consumers resulting from defendants' violations, including, but not limited to, rescission of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies.
- 63. 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: MA 31 , 2005

Respectfully submitted,

WILLIAM BLUMENTHAL General Counsel

Robert S. Kaye

Julie G. Bush

Attorneys for the Federal Trade Commission 600 Pennsylvania Ave., NW, Room 238

Washington, D.C. 20580

(202) 326-2215 (Kaye)

(202) 326-3608 (Bush)

(202) 326-3395 FACSIMILE





The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON THE REVERSE OF THE FORM.)

| the civil docket sheet (SEE II | NSTRUCTIONS ON THE REVE | ERSE OF THE FORM.) | • | | court for the purpose of militaring |
|--|--|--|--|--|--|
| I. (a) PLAINTIFFS | | | DEFENDANTS | | |
| Federal Trade Commission | on TIN-SE/ | ALED PE | Trust Soft, Inc., d | l/b/a SwankSoft and Sny | Killer; Danilo Ladendorf, |
| | 014 5000 | | individually and | as an officer of TrustSol | it. Inc. |
| (b) County of Residence | of First Listed Plaintiff | U.S. PLAINTIFF | - | of First Listed Defendant | Harris |
| | EXCEPT IN USAPLAINTHEF CA | | County of Residence | (IN U.S PLAINTIFF CASES | |
| , | Sealled | | NOTE IN LAN | ID CONDEMNATION CASES II | SE LINITED STATES COURTS |
| 1 | Public and unofficial s | taff access | | INVOLVED. | SOUTHERN DISTRICT OF TEXAS |
| | to this instrumen | | | | FILED |
| (c) Attorney's (Firm Name | . Address land illelephone chumbe | porder. | Attorneys (If Known) | | MAY 9 1 000F |
| Robert S. Kaye, Esq., Fee | | • | | 1905 | MAY 3 1 2005 |
| Avenue, N.W., Room 23: II. BASIS OF JURISE | | | | PRINCIPAL PARTIES | Michael NoMilby Clerk of Cour |
| _ | rection (mace and A m | i One Box Only) | (For Diversity Cases Only) | RINCHADIARIES | and One Box for Defendant) |
| ☑ 1 U.S. Government Plaintiff | 3 Federal Question | Mas a Danto | | TF DEF | PTF DEF |
| riammi | (U.S Government | (Not a Party) | Citizen of This State | I I I Incorporated or Proof Business In Th | |
| 7 | a | | | | |
| 2 U.S. Government Defendant | 4 Diversity | | Citizen of Another State | D 2 Incorporated and of Business In | |
| | (Indicate Citizensh | nip of Parties in Item III) | | of Dusiness III | Another State |
| | | | , | 3 G 3 Foreign Nation | □ 6 □ 6 |
| IV. NATURE OF SUI | T (N N) 0 0 0 | t . | Foreign Country | | |
| CONTRACT | | | ** FORFEITURE/PENALTY | BANKRUPTCY - 3 to | TESS OTHER STATUTES TO |
| ☐ 110 Insurance | PERSONAL INJURY | PERSONAL INJUR | | ☐ 422 Appeal 28 USC 158 | ☐ 400 State Reapportionment |
| 120 Marine | ☐ 310 Airplane | ☐ 362 Personal Injury | | 423 Withdrawal | 410 Antitrust |
| 130 Miller Act | 315 Airplane Product | Med. Malpractice | ☐ 625 Drug Related Seizure | 28 USC 157 | 430 Banks and Banking |
| ☐ 140 Negotiable Instrument ☐ 150 Recovery of Overpayment | Luability 320 Assault, Libel & | ☐ 365 Personal Injury - Product Liability | of Property 21 USC 881 630 Liquor Laws | - PROPERTY RIGHTS | 450 Commerce 460 Deportation |
| & Enforcement of Judgment | Slander | 368 Asbestos Persona | | ☐ 820 Copyrights | 470 Racketeer Influenced and |
| ☐ 151 Medicare Act | ☐ 330 Federal Employers' | Injury Product | ☐ 650 Airline Regs | ☐ 830 Patent | Corrupt Organizations |
| ☐ 152 Recovery of Defaulted Student Loans | Liability 340 Marine | Liability PERSONAL PROPER | ☐ 660 Occupational | ☐ 840 Trademark | 480 Consumer Credit |
| (Excl. Veterans) | 345 Marine Product | 370 Other Fraud | TY Safety/Health 690 Other | | ☐ 490 Cable/Sat TV ☐ 810 Selective Service |
| ☐ 153 Recovery of Overpayment | Liability | 371 Truth in Lending | LABOR | SOCIAL SECURITY | |
| of Veteran's Benefits 160 Stockholders' Suits | 350 Motor Vehicle | 380 Other Personal | ☐ 710 Fair Labor Standards | ☐ 861 HIA (1395ff) | Exchange |
| 190 Other Contract | 355 Motor Vehicle Product Liability | Property Damage 385 Property Damage | Act 720 Lubor/Mgmt, Relations | ☐ 862 Black Lung (923) ☐ 863 DIWC/DIWW (405(g)) | 875 Customer Challenge 12 USC 3410 |
| ☐ 195 Contract Product Liability | ☐ 360 Other Personal | Product Liability | ☐ 730 Labor/Mgmt.Reporting | ☐ 864 SSID Title XVI | 890 Other Statutory Actions |
| 196 Franchise | Injury | | & Disclosure Act | ☐ 865 RSI (405(g)) | ☐ 891 Agricultural Acts |
| □ 210 Land Condemnation | CIVIL RIGHTS 441 Voting | PRISONER PETITION 510 Motions to Vacat | - | ☐ 870 Taxes (U.S. Plaintiff | 892 Economic Stabilization Act 893 Environmental Matters |
| 220 Foreclosure | 442 Employment | Sentence | 790 Gulet Labor Engation 791 Empl. Ret. Inc. | or Defendant) | 894 Energy Allocation Act |
| 230 Rent Lease & Ejectment | 443 Housing/ | Habeas Corpus: | Security Act | ☐ 871 IRS—Third Party | 895 Freedom of Information |
| 240 Torts to Land 245 Tort Product Liability | Accommodations 444 Welfare | 530 General | # # # | 26 USC 7609 | Act |
| 290 All Other Real Property | 444 Welfare 445 Amer. w/Disabilities - | 535 Death Penalty 540 Mandamus & Oth | ner | | Under Equal Access |
| | Employment | 550 Civil Rights | | | to Justice |
| | 446 Amer. w/Disabilities - | 555 Prison Condition | | | ☐ 950 Constitutionality of |
| | Other 440 Other Civil Rights | | | | State Statutes |
| | - 440 Outer Civil Rights | | | <u> </u> | |
| V. ORIGIN (Place | an "X" in One Box Only) | | ••• | c 10 | Appeal to District |
| Ø1 Original □2 R | temoved from | Remanded from | | ferred from | rict D 7 Judge from Magistrate |
| | tate Court | Appellate Court | Reopened (speci | ify) Litigation | |
| | Cite the U.S. Civil Str | atute under which you ar | e filing (Do not cite jurisdiction: | al statutes unless diversity). | |
| VI. CAUSE OF ACTIO | DN Brief description of ca | | | | |
| | Unfair or decepti | ve practices in com | merce. | | |
| VII. REQUESTED IN | | IS A CLASS ACTION | | CHECK YES only | if demanded in complaint: |
| COMPLAINT: | UNDER F.R C.P. | | DEMAND 5 | JURY DEMAND: | · |
| | | | | JUNT DEMIAND: | Tes WNo |
| VIII. RELATED CASE | E(S) | | | | |
| IF ANY | (See instructions). | JUDGE | • | DOCKET NUMBER | |
| DATE | | SIGNATURE | TORNEY OF RECORD | | |
| DATE TALK | | SIGNATURE AT | OKNEY OF KECORD | | |
| 3/31/03 | 7 | Juli | X | | |
| FOR OFFICE USE ONLY | | <i></i> | | | |
| | | | | | |
| RECEIPT # A | MOUNT | APPLYING IFP | HIDGE | MAG HIT | ice. |