

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA

FEDERAL TRADE COMMISSION, and the

STATE OF ALABAMA,

Plaintiffs,

v.

TROTHSOLUTIONS INC., an Alabama corporation, also
d/b/a Troth Solutions,

TROTHSOLUTIONS LLC, a Nevada limited liability
company, also d/b/a Troth Solutions and
Trothsolutiontechnologies,

QUICKKONTO LLC, a Florida limited liability company,
also d/b/a Troth Solutions, Troth Av, Trothsolutions Av,
qkontos.com, Qkontos, Inc., and Qkontos, LLC,

CRAZY BEE MAN OF PALM BEACH INC., a Florida
corporation, also d/b/a Elfinam,

EDOORWAYS INTERNATIONAL CORP, a Florida
corporation, also d/b/a Trothsolutions,

ESCUE ENERGY, INC., a Nevada corporation, f/k/a
Edoorways International Corporation, also d/b/a
Trothsolutions and Trothsolution,

AIROWAYS LLC, a Nevada limited liability company,

MADHU SETHI, individually and as an officer of
QUICKKONTO LLC, CRAZY BEE MAN OF PALM
BEACH INC., EDOORWAYS INTERNATIONAL
CORP, and ESCUE ENERGY, INC., also d/b/a
Trothsolutiontechnologies, and

ILA SETHI, individually and as an officer of
TROTHSOLUTIONS INC. and TROTHSOLUTIONS
LLC,

Defendants.

Case No. _____

**COMPLAINT FOR PERMANENT
INJUNCTION AND OTHER
EQUITABLE RELIEF**

Plaintiffs, the Federal Trade Commission (“FTC”) and the State of Alabama, for their Complaint allege:

1. The FTC brings this action under Section 13(b) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 53(b), to obtain temporary, preliminary, and permanent injunctive relief, rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten monies, and other equitable relief for Defendants’ acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and in violation of the FTC’s Telemarketing Sales Rule (“TSR”) 16 C.F.R. Part 310, as amended.

2. The State of Alabama, by and through its Attorney General, Steven T. Marshall, brings this action under the Alabama Deceptive Trade Practices Act (DTPA), Ala. Code §§ 8-19-1 *et seq.*, to obtain temporary, preliminary and permanent injunctive relief, rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten monies, and other equitable relief, as well as civil penalties, for Defendants’ acts or practices in violation of the Alabama DTPA. The State of Alabama has conducted an investigation, and the head of the enforcing authority, Attorney General Steven T. Marshall, has determined that defendants will continue practices unlawful under the Alabama DTPA even if given an opportunity to appear before the Attorney General under § 8-19-8(a) of the Code of Alabama.

JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a), 53(b), 6102(c), and 6105(b).

4. This Court has supplemental jurisdiction over the State of Alabama’s claims pursuant to 28 U.S.C. § 1367.

5. Venue is proper in this district under 28 U.S.C. § 1391(b)(2)-(3), (c)(1)-(2) and (d), and 15 U.S.C. § 53(b).

PLAINTIFFS

6. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The FTC enforces 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 FTC also enforces the Telemarketing Act, 15 U.S.C. §§ 6101-6108, as amended. Pursuant to the Telemarketing Act, the FTC promulgated and enforces the TSR, 16 C.F.R. Part 310, as amended, which prohibits deceptive and abusive telemarketing acts or practices. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and the TSR, and to secure such equitable relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. §§ 53(b), 6102(c), and 6105(b).

7. The State of Alabama is the enforcing authority under the Alabama DTPA pursuant to § 8-19-8(a) of the Code of Alabama and is authorized to pursue this action to enjoin violations of the Alabama DTPA and to obtain legal, equitable or other appropriate relief, including rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten monies, civil penalties, or other relief as available under the Act.

DEFENDANTS

Corporate Defendants

8. Defendant Trothsolutions Inc., also doing business as Troth Solutions, is an Alabama corporation with its principal places of business at 85 Bagby Drive, Birmingham,

Alabama, and 181 W. Valley Ave., Suite 105, Birmingham, Alabama. Trothsolutions Inc. transacts or has transacted business in this district and throughout the United States. At times material to this Complaint, acting alone or in concert with others, Trothsolutions Inc. has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

9. Defendant Trothsolutions LLC, also doing business as Troth Solutions and Trothsolutionstechnologies, is a Nevada limited liability company with its principal places of business at 85 Bagby Drive, Birmingham, Alabama, 181 W. Valley Ave., Suite 105, Birmingham, Alabama, 22423 Overture Circle, Boca Raton, Florida, and 20423 SR 7, STE F-6495, Boca Raton, Florida. Trothsolutions LLC transacts or has transacted business in this district and throughout the United States. At times material to this Complaint, acting alone or in concert with others, Trothsolutions LLC has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

10. Defendant Quickkonto LLC, also doing business as Troth Solutions, Troth Av Trothsolutions Av, qkontos.com, Qkontos, Inc., and Qkontos, LLC, is a Florida limited liability company with its principal places of business at 22423 Overture Circle, Boca Raton, Florida, and 20423 SR 7, STE F-6495, Boca Raton, Florida. Quickkonto LLC transacts or has transacted business in this district and throughout the United States. At times material to this Complaint, acting alone or in concert with others, Quickkonto LLC has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

11. Defendant Crazy Bee Man of Palm Beach Inc., also doing business as Elfinam, is a Florida corporation with its principal place of business at 22423 Overture Circle, Boca Raton, Florida. Crazy Bee Man of Palm Beach Inc. transacts or has transacted business in this district and throughout the United States. At times material to this Complaint, acting alone or in concert with others, Crazy Bee Man of Palm Beach Inc. has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

12. Defendant Edoorways International Corp, also doing business as Trothsolutions, is a Florida corporation with its principal place of business at 22423 Overture Circle, Boca Raton, Florida. Edoorways International Corp transacts or has transacted business in this district and throughout the United States. At times material to this Complaint, acting alone or in concert with others, Edoorways International Corp has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

13. Defendant Escue Energy, Inc., formerly known as Edoorways International Corporation, also doing business as Trothsolutions and Trothsolution, is a Nevada corporation with its principal places of business at 22423 Overture Circle, Boca Raton, Florida, 11903 Southern Boulevard, Suite 108, Royal Palm Beach, Florida, and 85 Bagby Drive, Birmingham, Alabama. Escue Energy, Inc. transacts or has transacted business in this district and throughout the United States. At times material to this Complaint, acting alone or in concert with others, Escue Energy, Inc. has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

14. Defendant Airoways LLC is a Nevada limited liability company with its principal place of business at 22423 Overture Circle, Boca Raton, Florida. Airoways LLC transacts or has transacted business in this district and through the United States. At times material to this Complaint, acting alone or in concert with others, Airoways LLC has advertised, marketed, distributed, or sold computer technical support services and security software to consumers throughout the United States.

Individual Defendants

15. Defendant Madhu Sethi, also doing business as Trothsolutionstechnologies, is an owner, officer, director, member, or manager of corporate defendants Quickkonto LLC, Crazy Bee Man of Palm Beach Inc., Edoorways International Corp, and Escue Energy, Inc. At all times material to this Complaint, acting alone or in concert with others, he has formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint. Defendant Madhu Sethi has organized and created three of the corporate defendants, established and maintained bank accounts and merchant processing accounts, registered domain names, and procured other services used to facilitate Defendants' telemarketing scheme. He has responded to consumer complaints and has corresponded with the Better Business Bureau on behalf of Troth Solutions, and in such correspondence has referred to himself as the "manager" and "owner" of Troth Solutions. In connection with the matters alleged herein, Defendant Madhu Sethi transacts or has transacted business in this district and throughout the United States.

16. Defendant Ila Sethi is an owner, officer, director, member, or manager of corporate defendants Trothsolutions Inc. and Trothsolutions LLC. At all times material to this

Complaint, acting alone or in concert with others, she has formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint. Defendant Ila Sethi has organized and created corporate defendants Trothsolutions Inc. and Trothsolutions LLC, established and maintained bank accounts and merchant processing accounts, and registered domain names used to facilitate Defendants' telemarketing scheme. In connection with the matters alleged herein, Defendant Ila Sethi transacts or has transacted business in this district and throughout the United States.

Common Enterprise

17. Defendants Trothsolutions Inc., Trothsolutions LLC, Quickkonto LLC, Crazy Bee Man of Palm Beach Inc., Edoorways International Corp, Escue Energy, Inc., and Airoways LLC (collectively, "Corporate Defendants") have operated as a common enterprise while engaging in the deceptive acts and practices alleged below. Corporate Defendants have conducted the business practices described below through an interrelated network of companies that have common ownership, officers, managers, business functions, employees, and office locations, and that commingled funds. They share mailing addresses, business websites, telephone numbers, and marketing materials when soliciting consumers and communicating with third parties. Because these Corporate Defendants have operated as a common enterprise, each of them is jointly and severally liable for the acts and practices alleged below. Defendants Madhu and Ila Sethi have each formulated, directed, controlled, had the authority to control, or participated in the acts and practices of the Corporate Defendants that constitute the common enterprise.

COMMERCE

18. At all times material 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, and the Code of Alabama § 8-19-3(8).

DEFENDANTS’ BUSINESS ACTIVITIES

Overview

19. Defendants operate a scheme that deceives consumers into purchasing computer technical support services and security software to address alleged problems without any indication that such problems exist. Defendants carry out their scheme by misrepresenting that consumers’ computers are infected with viruses, malware, adware, or are otherwise compromised, and by falsely claiming to be authorized or certified by well-known technology companies, such as Microsoft or Apple, to service those companies’ products. Defendants initiate contact with consumers either through outbound cold calling or through deceptive pop-up advertisements that trick consumers into calling Defendants’ boiler rooms. Defendants’ conduct has generated dozens of complaints from defrauded consumers, many of whom are elderly, and caused millions of dollars in harm.

Defendants’ Outbound Calls and Pop-up Advertisement Campaign

20. From approximately May 2014 to February 2015, Defendants cold called consumers throughout the United States claiming to be from or affiliated with well-known technology companies such as Microsoft. During these telephone calls, Defendants typically claimed that consumers’ computers had been compromised by hackers, viruses, malware, adware, or some other vulnerability.

21. From approximately March 2015 to the present, Defendants have caused pop-up messages to be displayed on consumers' computers while consumers are browsing the internet. These pop-ups are typically designed so that consumers are unable to close or navigate around them, rendering consumers' web browsers unusable. This practice is known as "browser hijacking."

22. Defendants' pop-ups are designed to appear as if they originated from the computer's operating system, and often represent that they are messages from Microsoft, Apple, or another well-known technology company. The pop-ups claim that a serious technical or security issue has been identified with the consumer's computer, such as a virus, malware, adware, or other vulnerability. The pop-ups urge consumers to call a particular toll-free number immediately to resolve the issue. Often a loud alarm warning of the security risk accompanies the pop-up.

23. In some instances, Defendants cause a consumer's computer to simultaneously display several overlapping pop-up windows featuring various warnings about viruses and the imminent deletion of the computer's hard drive. The largest of these pop-ups prominently displays the Microsoft Windows logo along with the message "Hard Drive Safety Delete Starting In 4:59." This warning, which features a five minute timer that begins running when the pop-up first opens, is accompanied by similar alerts in overlapping pop-up windows, one of which states:

Your system might be infected with the adware_pop.exe computer virus. As such, your internet banking information could have been stolen.

Access to the internet has been blocked to protect your information until you fix this issue.

You are strongly advised to call the certified Tech Support office at 866-407-1560 now for IMMEDIATE assistance... You have virus infection! [sic] Please call Microsoft Certified Support Now!

The other pop-up window states:

Your Hard drive will be DELETED if you close this page. You have a Koobface virus. Please call the toll free [sic] for a free DIAGNOSIS.

See full screen Image A and enlarged Images A1 and A2 below.



(Image A)



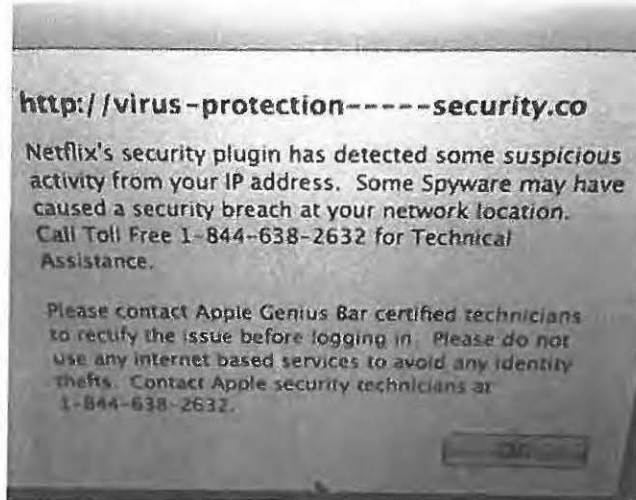
(Image A1)



(Image A2)

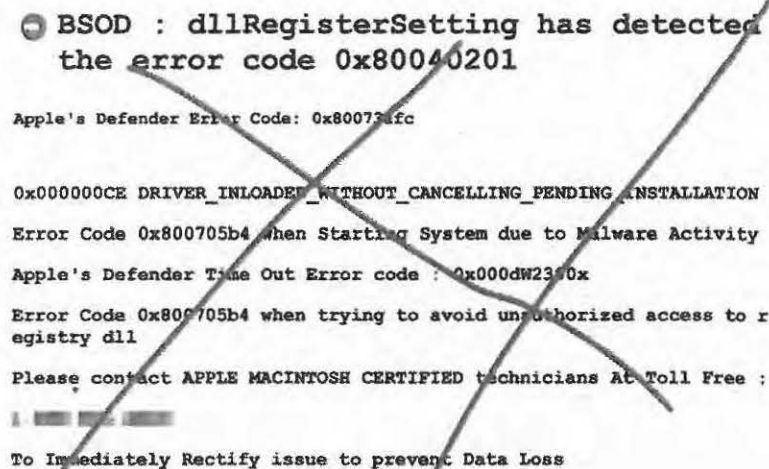
24. Some consumers receive a pop-up from Defendants claiming that “Netflix’s security plugin has detected some suspicious activity from your IP address” and directs consumers to “contact Apple Genius Bar certified technicians to rectify the issue before logging

in.” To “avoid any identity thefts [sic],” the popup advises consumers to “[c]ontact Apple security technicians at 1-844-638-2632.” See Image B below.



(Image B)

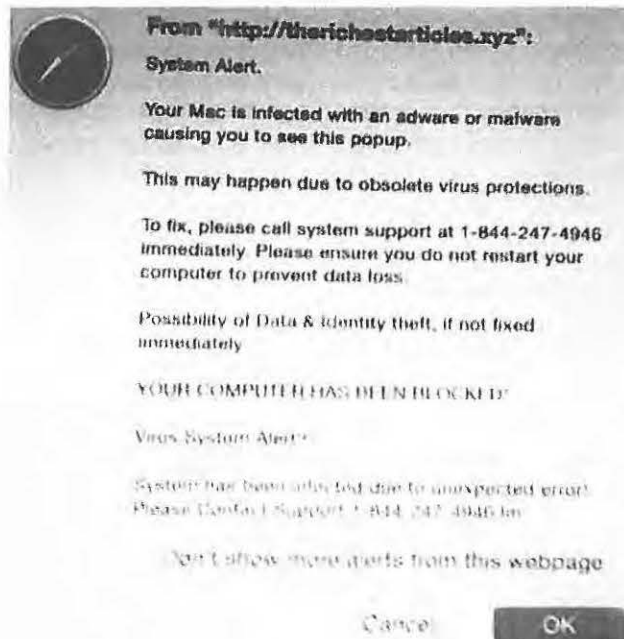
25. Other pop-ups used by Defendants warn about various “error codes” caused by “Malware Activity” and urge consumers to “contact APPLE MACINTOSH CERTIFIED technicians...To Immediately Rectify issue to prevent Data Loss.” See Image C below.



(Image C)

Defendants provided this image (with the visible markings) in response to a request from the Better Business Bureau for a copy of the pop-up advertisements that Defendants display to consumers.

26. Yet another pop-up used by Defendants claims to be a “Virus System Alert!!” informing consumers that their “Mac is infected with an adware or malware” that “may” be caused by “obsolete virus protections.” This pop-up, which features the Apple Safari logo, directs consumers to “fix” their computers by calling “system support at 1-844-247-4946 immediately” and warns that restarting could result in “data loss.” See Image D, below.



(Image D)

27. Defendants often display the pop-ups described in paragraphs 21 through 26 above to consumers whose computers do not have the virus, malware, adware, or other vulnerability Defendants claim they have. In many instances, Defendants claim affiliations with Microsoft, Apple, or other well-known technology companies. Defendants are not affiliated with

Microsoft, Apple, or other well-known technology companies.

Defendants Deceive Consumers into Buying Unnecessary Computer Technical Support Services and Security Software

28. Consumers who answer Defendants' cold calls or who place calls to the numbers contained in Defendants' pop-ups are connected with telemarketers employed by Defendants. Defendants' telemarketers then deliver a sales pitch designed to convince consumers that their computers are in urgent need of repair, even though Defendants have not detected an actual problem. For consumers calling in response to a pop-up message, Defendants' telemarketers typically begin their pitch by explaining that consumers receive the pop-up messages only if something is wrong with their computers.

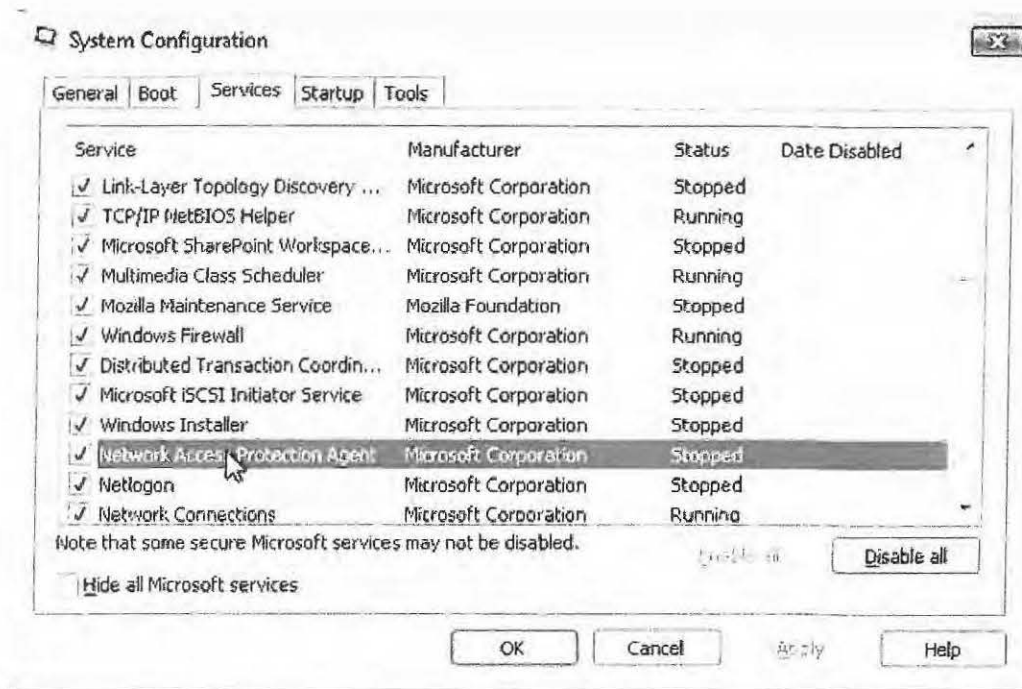
29. To gain consumers' trust, Defendants claim that they are affiliated with Microsoft or Apple, or otherwise certified or authorized by those companies to service their products. In fact, Defendants and their telemarketers are not affiliated with, or certified or authorized by, Microsoft or Apple. Moreover, Defendants' telemarketers are not qualified or authorized by Microsoft or Apple to diagnose problems with those companies' products.

30. After convincing consumers that the pop-ups signal serious problems that Defendants are qualified to diagnose and fix, Defendants' telemarketers tell consumers that they need to remotely access their computers to do so. The telemarketers typically direct consumers to a website from which Defendants' telemarketers can begin the remote access session. Once Defendants gain remote access, they are able to control the consumers' computers. Among other things, Defendants can view the computer screen, move the cursor, enter commands, run applications, and access stored information. At the same time, consumers can see what

Defendants are seeing and doing on their computers.

31. Once in control of consumers' computers, Defendants say they will run a series of purported diagnostic evaluations. In reality, these "diagnostics" are nothing more than a high-pressured sales pitch designed to scare consumers into believing that their computers are corrupted, hacked, or otherwise compromised. Defendants often use standard system information tools such as the System Configuration tool, Event Viewer, or the Command Prompt, each of which displays certain information about consumers' computers. Defendants misrepresent the technical significance of information from these tools, and in virtually every instance, claim to have identified performance or security problems on consumers' computers that must be resolved immediately. In many instances, Defendants claim that the "security" on consumers' computers has "expired" and must be renewed for a fee payable to Defendants.

32. A common ploy used by Defendants involves opening the Windows System Configuration tool and drawing consumers' attention to the number of "Stopped" services. In truth, it is normal for unnecessary Windows services to be designated as "Stopped." For example, Image E, below, is a screenshot taken during an undercover transaction that the FTC conducted with Defendants.



(Image E)

This screenshot shows the System Configuration tool opened by Defendants' telemarketer. According to the telemarketer, the information displayed in this window demonstrated that the computer's "Microsoft security softwares [sic]" had "expired" and had stopped functioning, allowing the computer to become infected with malware. In fact, the FTC computer used during this transaction was free of viruses, spyware, malware, or other security issues at the time of the undercover transaction. Moreover, the FTC's computer was running a free Microsoft security tool that does not expire or need to be renewed.

33. Another tactic frequently used by Defendants involves showing numerous "Error" and "Warning" messages in the Windows Event Viewer tool. In truth, these messages do not mean that a computer is infected with malware, is being hacked, or is otherwise compromised. It is normal for a Windows system to collect hundreds or thousands of "Error" or "Warning"

messages in the course of routine operations over time.

34. Yet another ploy used by Defendants involves manipulating the Windows Command Prompt application to run phony “scans” that produce equally phony error and warning messages. For example, Image F, below, is a screenshot taken during the FTC’s undercover transaction showing highlight marks made by Defendants’ telemarketer.

```

C:\Windows\system32\cmd.exe
601.18229 none 68d28a7192733a4d
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.18869 none 68abd625927398fb
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.18923 none 68c15ff922788e54
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.18973 none 68c146139289aa45
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.18939 none 68c747cf927b4241
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.19135 none 68c328af927f18d5c
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.21728 none 695ac552ab919bbb
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.22091 none 69b7efc6abd8db81
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.22125 none 6957a248ab997a6d
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.22177 none 69239348abbb38d9
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.22436 none 694dd858ab9ba72a
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.22654 none 69353b6cabac8d95
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.23072 none 691e7928abbd6c77
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.24126 none 69588baab93ad65
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.24136 none 694dbbdeab9bc955
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.23142 none 691eeacaaba72f6h
        amd64_microsoft_windows_microsoft_corporation_microsoft_corporation_31bf3856ad364e35_6.1.7
601.23338 none 694fc93eab991652
        C
C:\>tree
'tree' is not recognized as an internal or external command,
operable program or batch file.
C:\>tree
Security expired
'tree' is not recognized as an internal or external command,
operable program or batch file.
C:\>tree
network backed
'tree' is not recognized as an internal or external command,
operable program or batch file.

```

(Image F)

This screenshot shows the Command Prompt screen opened by the telemarketer, who typed “TREE,” causing lines of text to scroll down the screen for several seconds. The telemarketer claimed that this was a “quick Microsoft scan.” In fact, the TREE command simply displays a graphical representation of the computer’s directory tree. It does not scan for performance or security problems. Nevertheless, the telemarketer claimed that this “scan” had identified two

problems: “security expired” and “network hacked.” In reality, these words appeared because the telemarketer manually typed them, not because he had detected actual problems with the computer’s security or network.

35. After convincing consumers that their computers are in urgent need of repair, Defendants offer to remotely provide needed repairs as well as a “software warranty & security” service as an “additional benefit.” Depending on the length of the warranty selected by the consumer and the number of computers “repaired,” Defendants charge from \$200 to a thousand dollars or more. For example, during the undercover transaction conducted by Plaintiffs, Defendants charged \$500 for services even though the computer used during this transaction was free of viruses, spyware, malware, or other security or performance issues.

36. Consumers who do not agree, or hesitate, to pay for the security and technical support services Defendants recommend are subjected to intense pressure. Defendants’ telemarketers will, for example, warn such consumers that by failing to purchase the recommended services, their sensitive personal and financial information will be exposed to hackers.

37. If a consumer agrees to pay, Defendants’ telemarketers ask the consumer for a credit card or bank account number. After obtaining consumers’ credit card or bank account information, Defendants spend between thirty minutes to two hours performing the purported “repairs.” In numerous instances, these “repairs” are unnecessary or even harmful. At best, Defendants leave consumers’ computers in no worse condition than when the consumers first called Defendants. At worst, Defendants’ services may cause consumers’ computers to be more vulnerable to security incursions and other technical problems. For example, the proprietary

security software often installed by Defendants onto consumers' computers is identified as malware by four popular antivirus products.

VIOLATIONS OF THE FTC ACT

38. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits “unfair or deceptive acts or practices in or affecting commerce.”

39. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

**Count I
Defendants' Deceptive Misrepresentations About Affiliations
(By Plaintiff FTC)**

40. In numerous instances, in connection with the marketing, offering for sale, or selling of computer technical support services and security software, Defendants represent or have represented, directly or indirectly, expressly or by implication, through a variety of means, including telephone calls and internet communications, that they are part of or affiliated with well-known U.S. technology companies, such as Microsoft or Apple, or are certified or authorized by these companies to service their products.

41. In truth and in fact, Defendants are not part of or affiliated with these U.S. technology companies, nor are Defendants certified or authorized to service their products.

42. Therefore, Defendants' representations as set forth in Paragraph 40 of this Complaint are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count II
Defendants' Deceptive Misrepresentations About Security or Performance Issues
(By Plaintiff FTC)

43. In numerous instances, in connection with the marketing, offering for sale, or selling of computer technical support services and security software, Defendants represent or have represented, directly or indirectly, expressly or by implication, through a variety of means, including telephone calls and internet communications, that they have detected security or performance issues on consumers' computers, including system errors, viruses, spyware, malware, or the presence of hackers.

44. In truth and in fact, in numerous instances in which Defendants have made the representations set forth in Paragraph 43, Defendants have not detected security or performance issues on consumers' computers.

45. Therefore, Defendants' representations as set forth in Paragraph 43 are false, misleading, or were not substantiated at the time they were made and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

VIOLATIONS OF THE TELEMARKETING SALES RULE

46. Congress directed the FTC to prescribe rules prohibiting abusive and deceptive telemarketing acts or practices pursuant to the Telemarketing Act, 15 U.S.C. §§ 6101-6108, in 1994. The FTC adopted the original Telemarketing Sales Rule in 1995, extensively amended it in 2003, and amended certain provisions thereafter.

47. Defendants are "sellers" or "telemarketers" engaged in "telemarketing" as defined by the TSR, 16 C.F.R. § 310.2(dd), (ff), and (gg).

48. The TSR prohibits any seller or telemarketer from making a false or misleading statement to induce any person to pay for goods or services or to induce a charitable contribution. 16 C.F.R. § 310.3(a)(4).

49. Pursuant to Section 3(c) of the Telemarketing Act, 15 U.S.C. § 6102(c), and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the TSR constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count III
Deceptive Telemarketing Calls in Violation of the TSR
(By Both Plaintiffs)

50. In numerous instances, in connection with telemarketing their goods and services, Defendants have made false or misleading statements, directly or by implication, to induce consumers to pay for goods or services, including, but not limited to, misrepresentations that Defendants are part of well-known U.S. technology companies, such as Microsoft or Apple, or are certified or authorized by these companies to service their products.

51. Defendants' acts or practices, as described in Paragraph 50, are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(a)(4).

Count IV
Deceptive Telemarketing Calls in Violation of the TSR
(By Both Plaintiffs)

52. In numerous instances, in connection with telemarketing their goods and services, Defendants have made false or misleading statements, directly or by implication, to induce consumers to pay for goods or services, including, but not limited to, misrepresentations that

Defendants have detected security or performance issues on consumers' computers, including system errors, viruses, spyware, malware, or the presence of hackers.

53. Defendants' acts or practices, as described in Paragraph 52 above, are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(a)(4).

VIOLATIONS OF THE ALABAMA DECEPTIVE TRADE PRACTICES ACT

54. Section 8-19-5 of the Alabama DTPA prohibits "deceptive acts or practices in the conduct of any trade or commerce."

**Count V
Alabama Deceptive Trade Practices Act Violation
(By State of Alabama)**

55. In numerous instances, in connection with the marketing, offering for sale, or selling of computer security and technical support services, Defendants represent or have represented, directly or indirectly, expressly or by implication, through a variety of means, including through telephone calls and internet communications, that Defendants are part of well-known U.S. technology companies, such as Microsoft or Apple, or are certified or authorized by these companies to service their products.

56. The Alabama DTPA prohibits "[c]ausing confusion or misunderstanding as to the affiliation, connection, or association with, or certification by another." § 8-19-5(3).

57. In truth and in fact, Defendants are not part of or affiliated with these U.S. technology companies, nor are Defendants certified or authorized to service their products.

58. Defendants' representations as set forth in Paragraph 55 are false and "[c]aus[ed] confusion or misunderstanding as to the affiliation, connection, or association with, or certification by another" in violation of § 8-19-5(3).

Count VI
Alabama Deceptive Trade Practices Act Violation
(By State of Alabama)

59. In numerous instances, in connection with the marketing, offering for sale, or selling of computer security and technical support services, Defendants represent or have represented, directly or indirectly, expressly or by implication, through a variety of means, including through telephone calls and internet communications, that they have detected security or performance issues on consumers' computers, including system errors, viruses, spyware, malware, or the presence of hackers.

60. The Alabama DTPA prohibits "[e]ngaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct or trade or commerce." § 8-19-5(27).

61. In truth and in fact, in instances in which Defendants have made the representations set forth in Paragraph 59, Defendants have not detected security or performance issues on consumers' computers that necessitate repair service.

62. Defendants' representations as set forth in Paragraph 59 demonstrate that Defendants have "[e]ngag[ed] in any other unconscionable, false, misleading, or deceptive act[s] or practice[s] in the conduct of trade or commerce" in violation of § 8-19-5(27).

CONSUMER INJURY

63. Consumers have suffered and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act, the TSR, and the Alabama DTPA. In addition, Defendants have been unjustly enriched as a result of their unlawful acts or practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

64. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

65. Pursuant to 28 U.S.C. § 1367, this Court has supplemental jurisdiction to allow Plaintiff State of Alabama to enforce its state law claims against Defendants in this Court for violations of Alabama DTPA, including injunctive relief, the refund of monies paid, the disgorgement of ill-gotten monies, and civil penalties.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Sections 13(b) of the FTC Act, 15 U.S.C. §53(b), and the TSR; and Plaintiff State of Alabama, pursuant to § 8-19-8; and as authorized by the Court's own equitable powers, requests that the Court:

A. 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, including but not limited to, temporary and preliminary injunctions, and an order providing for immediate access, the turnover of business records, an asset freeze, the appointment of a receiver, and the disruption of domain and telephone services;

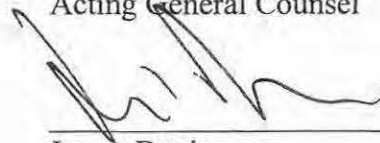
B. Enter a permanent injunction to prevent future violations of the FTC Act, the TSR, and Alabama DTPA by Defendants;

C. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act, the TSR, and the Alabama DTPA, including but not limited to, rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

D. Award Plaintiff FTC the costs of bringing this action, and Plaintiff State of Alabama its attorneys' fees and costs in bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

Respectfully submitted,

DAVID C. SHONKA
Acting General Counsel



James Davis
Elizabeth C. Scott
Federal Trade Commission, Midwest Region
55 West Monroe Street, Suite 1825
Chicago, Illinois 60603
jdavis@ftc.gov
escott@ftc.gov
(312) 960-5611 [Davis]
(312) 960-5609 [Scott]

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

Dated: _____

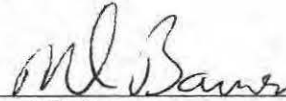
5/1/17

STEVEN T. MARSHALL
ATTORNEY GENERAL
STATE OF ALABAMA

by:

Dated: _____

5/1/17



Noel S. Barnes
Michael G. Dean
Assistant Attorneys General
Office of the Attorney General
501 Washington Avenue
Montgomery, AL 36104
nbarnes@ago.state.al.us
mdean@ago.state.al.us
(334) 353-9196

Attorneys for Plaintiff
STATE OF ALABAMA