LT

UNITED STATES DISTRICT COURT
FOR THE NORTHERN D

1:16-cv-06607
Judge John Robert Blakey
Magistrate Judge Mary M. Rowland

FEDERAL TRADE COMMISSION, and

OFFICE OF THE ATTORNEY GENERAL, STATE OF FLORIDA, DEPARTMENT OF LEGAL AFFAIRS

Plaintiffs,

v.

BIG DOG SOLUTIONS LLC, also d/b/a Help Desk National and Help Desk Global, a Florida limited liability company;

PC HELP DESK US LLC, also d/b/a Help Desk National and Help Desk Global, a Florida limited liability company,

INBOUND CALL SPECIALIST LLC, a Florida limited liability company,

BLACKOPTEK CE INC., a Nevada corporation,

9138242 CANADA CORPORATION, a Quebec, Canada corporation,

DIGITAL GROWTH PROPERTIES, LLC, an Iowa limited liability company,

CHRISTOPHER J. COSTANZA, individually and as an owner or officer of Big Dog Solutions LLC, PC Help Desk US LLC, and Inbound Call Specialist LLC, and also d/b/a CJM Consulting LLC,

SUZANNE W. HARRIS, individually and as an owner or officer of Big Dog Solutions LLC,

MUZAFFAR ABBAS, individually and as an owner or officer of 9138242 Canada Corporation and BlackOptek CE Inc.,

GARY OBERMAN, individually and as an owner or officer of 9138242 Canada Corporation,

[FILED UNDER SEAL]

COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF

FILED

JUN 24 2016

THOMAS G. BRUTON
CLERK, U.S. DISTRICT COURT

DONALD DOLPHIN, individually and as an owner or officer of BlackOptek CE Inc. and 9138242 Canada Corporation, and

JUSTIN POWERS, individually and as an owner or officer of Digital Growth Properties, LLC,

Defendants.

Plaintiffs, the Federal Trade Commission ("FTC") and the Office of the Attorney General, State of Florida, Department of Legal Affairs ("State of Florida") 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), and the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"), 15 U.S.C. §§ 6101-6108, as amended, 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 the 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.

2. The State of Florida, by and through its Attorney General, Pamela Jo Bondi, brings this action under the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), § 501.201, *et seq.*, Florida Statutes 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 FDUTPA. The State of Florida has conducted an investigation, and

the head of the enforcing authority, Attorney General Pamela Jo Bondi, has determined that an enforcement action serves the public interest.

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 Florida'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)(3), 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, which prohibits deceptive and abusive telemarketing acts or practices.

7. 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).

8. The State of Florida is the enforcing authority under the FDUTPA pursuant to Section 501.203(2), Florida Statutes, and is authorized to pursue this action to enjoin violations

of the FDUTPA 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, or other relief as may be appropriate. . §§ 501.207, 501.2075 and 501.2077, Florida Statutes.

DEFENDANTS

9. Defendant Big Dog Solutions LLC, also d/b/a Help Desk National and Help Desk Global ("Big Dog Solutions"), is a Florida limited liability company with its principal places of business at 10405 Willow Oaks Trail, Boynton Beach, Florida and 2240 West Woolbright Road, Suite 205, Boynton Beach, Florida. Big Dog Solutions transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, Big Dog Solutions has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

10. Defendant PC Help Desk US LLC, also d/b/a Help Desk National and Help Desk Global ("PC Help Desk"), is a Florida limited liability company with its principal places of business at 10405 Willow Oaks Trail, Boynton Beach, Florida and 2240 West Woolbright Road, Suite 205, Boynton Beach, Florida. PC Help Desk transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, PC Help Desk has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

11. Defendant Inbound Call Specialist LLC ("Inbound Call Specialist") is a Florida limited liability company with its principal places of business at 10405 Willow Oaks Trail, Boynton Beach, Florida and 2240 West Woolbright Road, Suite 205, Boynton Beach, Florida. Inbound Call Specialist transacts or has transacted business in this district and throughout the

United States. At all times material to this Complaint, acting alone or in concert with others, Inbound Call Specialist has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

12. Defendant BlackOptek CE Inc. ("BlackOptek") is a Nevada corporation with its principal places of business at 21 Daws Hare Crescent, Stouffville, Ontario, and 800 West El Camino Real, Suite 180, Mountainview, California. BlackOptek transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, BlackOptek has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

13. Defendant 9138242 Canada Corporation ("9138242 Canada") is a Canadian corporation with its principal place of business at Sherbrooke Street West, Suite 1900, Montreal, Quebec. 9138242 Canada transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, 9138242 Canada has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

14. Defendant Digital Growth Properties, LLC ("Digital Growth Properties") is an Iowa limited liability company with its principal place of business at 601 6th Street Northeast, Mitchellville, Iowa. Digital Growth Properties transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, Digital Growth Properties has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

15. Defendant Christopher J. Costanza, who also does business as CJM Consulting LLC, is an owner, officer, director, member, or manager of defendants Big Dog Solutions, PC

Help Desk US, and Inbound Call Specialist. 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 Costanza is responsible for organizing and creating corporate defendants Big Dog Solutions, PC Help Desk US, and Inbound Call Specialist, managing Defendants' call centers, establishing and maintaining corporate bank accounts, and procuring services used to facilitate Defendants' telemarketing scheme. In connection with the matters alleged herein, Defendant Costanza transacts or has transacted business in this district and throughout the United States.

16. Defendant Suzanne W. Harris is an owner, officer, director, member, or manager of defendant Big Dog Solutions. 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 Harris is a signatory on numerous corporate bank accounts held in Defendants' names and used in connection with the matters alleged herein. In connection with the matters alleged herein, Defendant Harris transacts or has transacted business in this district and throughout the United States.

17. Defendant Muzaffar Abbas is an owner, officer, director, member, or manager of defendants BlackOptek and 9138242 Canada. 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 Abbas is responsible for organizing and creating defendants BlackOptek and 9138242 Canada, establishing and maintaining corporate bank accounts held in those corporate defendants' names, and procuring services used to facilitate Defendants' telemarketing scheme. In connection with

the matters alleged herein, Defendant Abbas transacts or has transacted business in this district and throughout the United States.

18. Defendant Gary Oberman is an owner, officer, director, member, or manager of defendant 9138242 Canada. 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 Oberman is a signatory on numerous corporate bank accounts held in Defendants' names and used in connection with the matters alleged herein, and is responsible for procuring services used to facilitate Defendants' telemarketing scheme. In connection with the matters alleged herein, Defendant Oberman transacts or has transacted business in this district and throughout the United States.

19. Defendant Donald Dolphin is an owner, officer, director, member, or manager of defendants BlackOptek CE and 9138242 Canada. 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 Dolphin is a signatory on corporate bank accounts used in connection with the matters alleged herein and is responsible for procuring services used to facilitate Defendants' telemarketing scheme. In connection with the matters alleged herein, Defendant Dolphin transacts or has transacted business in this district and throughout the United States.

20. Defendant Justin Powers is an owner, officer, director, member, or manager of defendant Digital Growth Properties. 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 Powers is responsible for deceptive Internet advertising used to promote and generate leads for Defendants'

telemarketing scheme. In connection with the matters alleged herein, Defendant Powers transacts or has transacted business in this district and throughout the United States.

21. Defendants Big Dog Solutions, PC Help Desk US, Inbound Call Specialist, BlackOptek, and 9138242 Canada ("Help Desk National Defendants") have operated as a common enterprise while engaging in the deceptive and unlawful acts and practices and other violations of law alleged below. The Help Desk National Defendants have conducted the business practices described below through an interrelated network of companies that have common ownership, business functions, office locations and that have commingled funds. They share mailing addresses, business websites, telephone numbers, and marketing materials when soliciting consumers and dealing with third parties. Because the Help Desk National Defendants have operated as a common enterprise, each of them is jointly and severally liable for the acts and practices alleged below. Defendants Costanza, Harris, Abbas, Oberman, and Dolphin have 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

22. 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 Florida Statutes § 501.203(8).

DEFENDANTS' BUSINESS ACTIVITIES

Overview

23. Defendants operate a telemarketing scheme that deceives consumers into purchasing computer security or technical support services to address purported problems with their computers regardless of whether problems with their computers actually exist. Defendants

carry out their scheme by misrepresenting to consumers that their computers are infected, corrupted, hacked, or otherwise compromised, and by falsely claiming to be authorized by well-known technology companies, such as Microsoft and Apple, to service those companies' products. Since at least January 2015, Defendants have bilked millions of dollars from consumers, many of whom are senior citizens.

Defendants' Pop-up Warnings

24. Defendants cause pop-up messages ("pop-ups") to be displayed on consumers' computers instructing them to immediately call a toll free number for technical assistance. Consumers who dial these numbers are connected to Defendants' telemarketers in Boynton Beach, Florida.

25. In many instances, Defendants generate pop-ups that render consumers' web browser unusable, such that, when a consumer closes the pop-up, another, similar pop-up immediately reappears. In many instances, consumers are unable to close the pop-up completely, and the web browser appears to be disabled. This practice is known as "browser hijacking."

26. Defendants use a variety of ruses to lure consumers to the websites that generate these pop-ups. For example, Defendants drive traffic to websites through paid internet advertisements that appear in search results generated by search engines, such as Google. Some of these advertisements are placed by affiliate marketers who receive a commission from Defendants in return for leads that they generate.

27. Defendants' pop-ups warn consumers that their computers may be compromised by security threats and instruct them to call a toll free number listed in the message. The pop-ups are designed to appear as if they originated from a computer's operating system and often

mislead consumers into believing that they are receiving a message from Microsoft or Apple.

One of Defendants' pop-ups displays the message "WARNING – SECURITY ALERT" in the browser tab heading and contains the following statements:

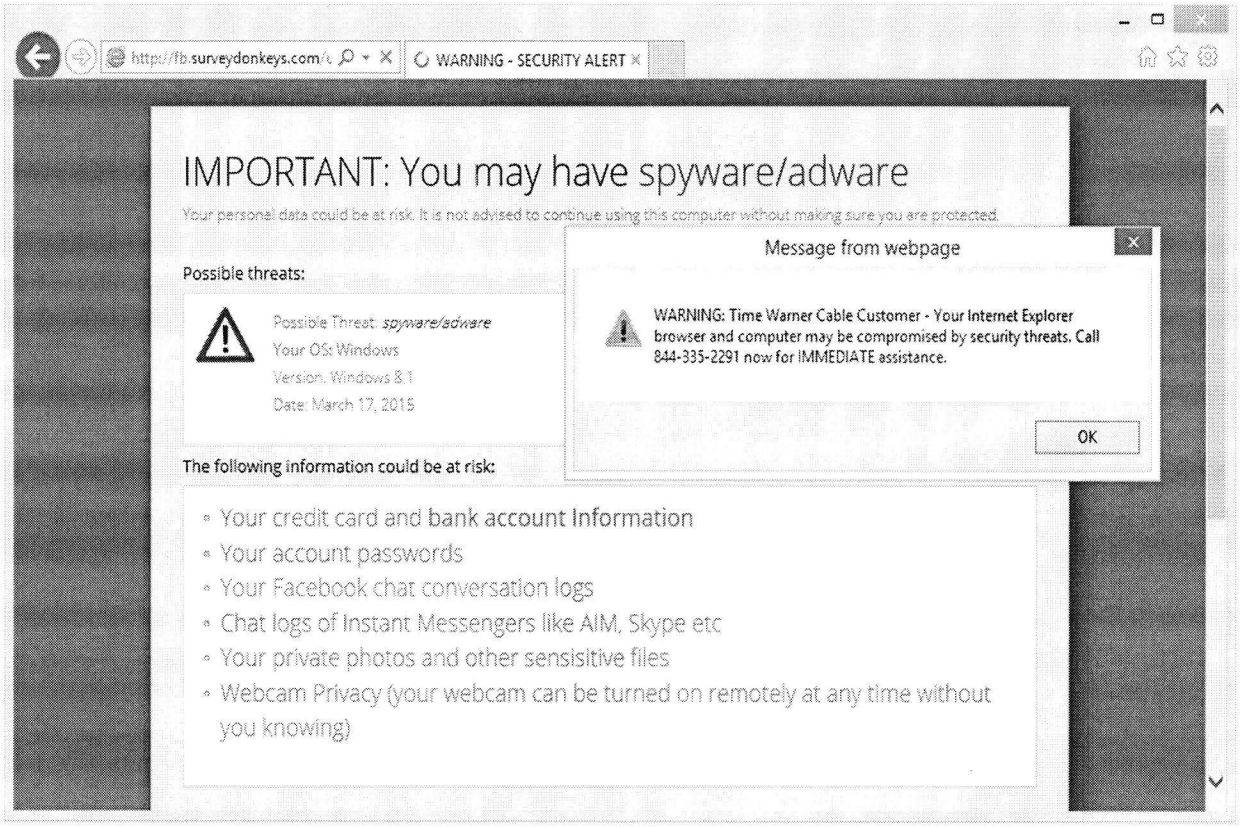
> WARNING: Time Warner Cable Customer – Your Internet Explorer browser and computer may be compromised by security threats. Call 844-355-2291 now for IMMEDIATE assistance.

A separate window accompanying this pop-up states:

> IMPORTANT: You may have adware/spyware
> Your personal data could be at risk. It is not advised to continue using this computer without making sure you are protected.
> ...
>
> The following information could be at risk:
>
> - Your credit card and **bank account information**
> - Your account passwords
> - Your Facebook chat conversation logs
> - Chat logs of Instant Messengers like AIM, Skype, etc.
> - Your private photos and other sensitive files
> - Webcam Privacy (your webcam can be turned on remotely at any time without you knowing)

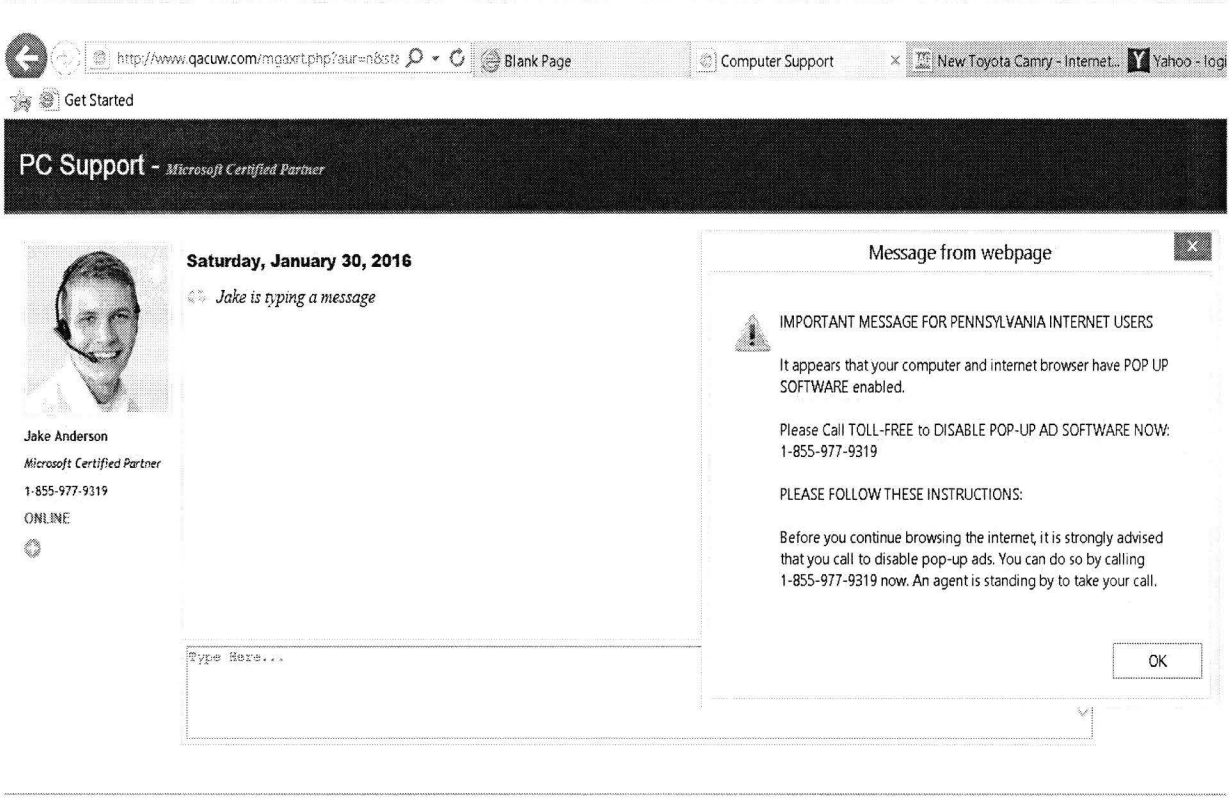
See Image 1 below. An audio recording accompanying this pop-up plays the following warning:

> Important security message: please call the number provided as soon as possible. You will be guided for the removal of any adware, spyware, or virus that is found on your computer. Seeing these messages means that you possibly have them installed on your computer, which puts the security of your personal data at a serious risk. It's strongly advised that you call the phone number provided and get your computer scanned before you continue using your Internet.



(Image 1)

28. In many instances, Defendants' pop-ups are accompanied by a separate window containing a so-called "chatbot" designed to trick consumers into believing that they are communicating with an individual who is either: (1) affiliated with, or employed by, Microsoft or Apple, or (2) certified to service Microsoft and Apple products. *See* Image 2 below. For example, Defendants' chatbot windows often depict an individual named "Jake Anderson," "Gregg Foster," or "Molly Jefferson," who is identified as a "Microsoft Certified Partner." *See* Image 2 below. Consumers who exchange messages with the chatbots are inevitably warned that their computers are compromised in some way, and they are urged to immediately call one of Defendants' toll-free numbers.



(Image 2)

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

29. Consumers who contact Defendants' call center after encountering a pop-up or chatbot are led through a scripted sales pitch designed to convince them that their computers are in urgent need of repair, even though Defendants have not detected that an actual problem exists. Defendants' telemarketers begin this deception by explaining why consumers' computers are displaying Defendants' pop-up warnings and chatbots. Defendants' telemarketers mislead consumers into believing that the pop-ups originate from within their computers' operating systems, "like the check engine light" on a car, and are generated when the computers detect a problem. Similarly, Defendants' sales script falsely characterizes the chatbots as "valuable tools to assess any risk or problems associated with your operating system."

30. To gain consumers' trust, Defendants claim that they are certified or authorized by Microsoft and Apple to service products manufactured by these companies. For example, Defendants' script instructs telemarketers to provide the following response to consumers who question Defendants' "credibility": "We are partnered with Microsoft [and] certified to service all Microsoft products [and] programs." In reality, Defendants are not certified or authorized by Microsoft to service Microsoft products. Similarly, Defendants are not certified or authorized by Apple to service Apple products. Moreover, Defendants' telemarketers are not qualified or authorized by Microsoft or Apple to diagnose problems with those companies' products.

31. After convincing consumers that the pop-ups indicate that there may be problems with their computers and that Defendants are qualified to diagnose those problems and fix them, Defendants' telemarketers tell consumers that they need to remotely access the consumers' computers to identify and resolve the problems. The telemarketers typically direct consumers to go to a website, enter a code, and follow the prompts to begin the remote access session. Once Defendants gain remote access, they are able to control the consumers' computers. For example, Defendants can view the computer screen, move the mouse or cursor, enter commands, run applications, and access stored information, among other things. At the same time, consumers can see what Defendants are seeing and doing on their computers.

32. Once in control of consumers' computers, Defendants run a series of purported diagnostic tests, which, in reality, are nothing more than a high-pressured sales pitch designed to scare consumers into believing that their computers are corrupted, hacked, otherwise compromised, or generally performing badly. For computers running versions of Microsoft Windows, these diagnostic tests often include displaying the computer's Task Manager, the Microsoft System Configuration Utility ("msconfig") services tab, and the msconfig start-up

menu. For computers running versions of Apple's OS X, these evaluations often include displaying the computer's activity monitor, system report information, and error reports appearing in the console log. For both Windows and Apple systems, Defendants also sometimes install a software program on the consumer's computer purportedly capable of identifying problems and assessing its "overall health."

33. Defendants misrepresent the technical significance of their diagnostic tests, and in virtually every instance, claim that the tests have identified performance or security problems on consumers' computers that require immediate repair.

34. To further alarm and defraud consumers, Defendants invariably claim that any security software currently running on consumers' computers is outdated and incapable of adequately protecting against the latest and most egregious threats.

35. After being misled into believing that their computers are compromised and in need of immediate repair, consumers are informed that they can bring their computers to a well-known retailer, such as Best Buy or Staples. However, Defendants warn that this option will be very costly, take several days to complete, and possibly expose consumers' computers to additional harm caused by incompetent or unscrupulous technicians. As an alternative, Defendants offer to repair consumers' computers remotely that same day while consumers sit in the comfort of their own home.

36. Defendants charge consumers approximately $200 to $400 for their technical support services. In many instances, Defendants use the fear they have created to sell their one-time repair services as a means of pushing an ongoing technical support plan ranging in price from approximately $9.99 per month to $19.99 per month. These recurring fees continue until consumers cancel the service.

37. In addition to convincing consumers they need to purchase technical support services, Defendants' telemarketers also attempt to upsell computer security software, such as Stopzilla, Defender Pro, Magnum Total Security, and others, at an inflated price. Even when consumers already have well-known computer security software installed on their computers, such as McAfee or AVG, Defendants insist that consumers need a more reliable alternative sold by Defendants. Defendants purchase licenses for these programs for $10 or less and resell them to consumers for several hundred dollars.

38. Consumers who do not agree, or hesitate, to pay for the computer security and technical support services recommended by Defendants are subjected to intense pressure. Defendants' telemarketers will, for example, warn such consumers that by failing to purchase the recommended software and services, they are likely to cause irreparable damage to their computers as well as expose sensitive personal and financial information about them and their families to hackers.

39. After charging consumers for computer security and technical support services, Defendants' telemarketers then transfer the consumer's remote access session to a purported technician to perform "repairs." In numerous instances, these "repairs" are unnecessary or harmful.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

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

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

COUNT I
Deceptive Misrepresentations
(By Plaintiff Federal Trade Commission)

42. 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 telephone calls and internet communications, that they 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.

43. In truth and in fact, Defendants are not part of these U.S. technology companies or are not certified or authorized to service their products.

44. Therefore, Defendants' representations set forth in Paragraph 42 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
Deceptive Misrepresentations
(By Plaintiff Federal Trade Commission)

45. 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 viruses, spyware, malware, or the presence of hackers.

46. In truth and in fact, in numerous instances in which the Defendants have made the representations set forth in Paragraph 45, Defendants have not detected security or performance issues on consumers' computers.

47. Therefore, Defendants' representations as set forth in Paragraph 45 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

48. 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.

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

50. 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).

51. The TSR's prohibition against making false or misleading statements applies to all statements regarding upsells, whether the statements were made during an outbound call initiated by the telemarketer or an inbound call initiated by a consumer. 16 C.F.R. §§ 310.2(ee), 310.6(4).

52. 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)

53. 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 certified or authorized by these companies to service their products.

54. Defendants' acts or practices, as described in Paragraph 53, 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)

55. 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 viruses, spyware, malware, or the presence of hackers.

56. Defendants' acts or practices, as described in Paragraph 55 above, are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(a)(4).

VIOLATIONS OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT

57. Section 501.204 of FDUTPA, Chapter 501, Part II, Florida Statutes, prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce."

COUNT V
Florida Deceptive and Unfair Trade Practices Act Violation
(By Plaintiff State of Florida)

58. As set forth in Paragraphs 1 through 39 above, which allegations are incorporated as if set forth herein, 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 viruses, spyware, malware, or the presence of hackers.

59. In truth and in fact, in numerous instances in which Defendants have made the representations set forth in Paragraph 58, Defendants have not detected security or performance issues on consumers' computers.

60. Defendants' representations as set forth in Paragraph 58 of this Complaint are false and misleading and likely to mislead consumers acting reasonably, and/or consumers within the State of Florida were actually misled by Defendants' misrepresentations in violation of Section 501.204 of FDUTPA.

COUNT VI
Florida Deceptive and Unfair Trade Practices Act Violation
(By Plaintiff State of Florida)

61. As set forth in Paragraphs 1 through 39 above, which allegations are incorporated as if set forth herein, 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 certified or authorized by these companies to service their products.

62. In truth and in fact, in numerous instances in which Defendants have made the representations set forth in Paragraph 61, Defendants are not part of these U.S. technology companies or are not certified or authorized to service their products.

63. Defendants' representations as set forth in Paragraph 61 of this Complaint are false and misleading and likely to mislead consumers acting reasonably, and/or consumers within the State of Florida were actually misled by Defendants' misrepresentations in violation of Section 501.204 of FDUTPA.

CONSUMER INJURY

64. Consumers have suffered and will continue to suffer substantial injury as a result of the Defendants' violations of the FTC Act, the TSR, and the FDUTPA. 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

65. 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.

66. Section 6(b) of the Telemarketing Act, 15 U.S.C. § 6105(b), authorizes this Court to grant such relief as the Court finds necessary to redress injury to consumers resulting from the Defendants' violations of the TSR, including the rescission or reformation of contracts, and the refund of money.

67. Pursuant to 28 U.S.C. § 1367, this Court has supplemental jurisdiction to allow Plaintiff State of Florida to enforce its state law claims against Defendants in this Court for violations of the FDUTPA. Florida Statutes Sections 501.207, 501.2075, and 501.2077 authorize this Court to grant such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violation of the FDUTPA, including injunctive relief, rescission or reformation of contracts, the refund of monies paid, the disgorgement of ill-gotten monies, and civil penalties.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. §§ 53(b), the TSR, and the Court's own equitable powers, and Plaintiff State of Florida, pursuant to Florida Statutes Sections 501.207, 501.2075, and 501.2077 and as authorized by the Court's own equitable powers, request that the Court:

A. Award Plaintiffs 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 FDUTPA by Defendants;

C. Award such relief as the Court finds necessary to redress injury to consumers resulting from the Defendants' violations of the FTC Act, the TSR and FDUTPA, 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 Florida 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.

Dated: June 24, 2016

Respectfully submitted,

DAVID C. SHONKA
Acting General Counsel

James Davis
Matthew H. Wernz
Federal Trade Commission, Midwest Region
55 West Monroe Street, Suite 1825
Chicago, Illinois 60603
jdavis@ftc.gov
mwernz@ftc.gov
(312) 960-5611 [Davis]
(312) 960-5596 [Wernz]

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

PAMELA JO BONDI
ATTORNEY GENERAL
STATE OF FLORIDA

/s/ Michelle Pardoll
Michelle Pardoll
Assistant Attorney General
Florida Bar No. 0073915
Michelle.Pardoll@myfloridalegal.com
110 S.E. 6th Street, 10th Floor
Fort Lauderdale, Florida 33301
Phone: (954) 712-4600

Attorney for Plaintiff
STATE OF FLORIDA