

IN THE CIRCUIT COURT OF THE
FIFTEENTH JUDICIAL CIRCUIT IN
PALM BEACH COUNTY, FLORIDA

[FILED UNDER SEAL]

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

Case No.: 50-2017-CA-004449

Plaintiff,

vs.

GOREADYCALLS MARKETING, LLC, *a Florida Limited Liability Company*; KRADANOMIC SOLUTIONS, LLC, *a Florida Limited Liability Company*; WIZARD TECH SOLUTIONS, LLC, *a Florida Limited Liability Company*; TEAMKEEN, LLC, *a Florida Limited Liability Company*; CUTTING EDGE OUTLOOK, LLC, *a Florida Limited Liability Company*; US SOFTWARE EXPERTS, LLC, *a Florida Limited Liability Company*; SECURE IT DIGITAL SOLUTIONS, LLC, *a Florida Limited Liability Company*; CAPITAL INVESTMENTS LLC, *a Florida Limited Liability Company*; A.E.A. WORLDWIDE LLC, *a Florida Limited Liability Company*; US SOFTWARE PROS LLC, *a Florida Limited Liability Company*; SOFTWARE PROS LLC, *a Florida Limited Liability Company*; ADAM LENNOX, *an Individual*; EVAN KEEN, *an Individual*

Defendants,

COMPLAINT

Plaintiff, Office of the Attorney General, State of Florida, Department of Legal Affairs, brings this action under the Florida Deceptive and Unfair Trade Practices Act (“FDUTPA”), Section 501.201 et seq., Florida Statutes, against GoReadyCalls Marketing, LLC (“**Lead Defendant**”); Kradanomic Solutions, LLC, Wizard Tech Solutions, LLC, TeamKeen, LLC,

Cutting Edge Outlook, LLC, US Software Experts, LLC, Secure IT Digital Solutions, LLC, Capital Investments LLC, A.E.A. Worldwide LLC, US Software Pros LLC, Software Pros LLC (“**Enterprise Defendants**”); and Adam Lennox and Evan Keen (“**Individual Defendants**”); (Lead Defendant, Enterprise Defendants, and Individual Defendants are collectively referred to as “**Defendants**”), to obtain preliminary and permanent injunctive relief, restitution, the imposition of civil penalties, an award of attorney’s fees, and other equitable relief, for Defendants’ acts or practices in violation of FDUTPA, and further states:

JURISDICTION AND VENUE

1. This action is brought pursuant to FDUTPA. This Court has jurisdiction pursuant to Section 26.012, Florida Statutes, and FDUTPA.
2. Defendants at all times material to this Complaint, acting alone or in concert with others, provided goods or services within the definition of Section 501.203(8), Florida Statutes, solicited consumers within the definition of Section 501.203(7), Florida Statutes, and were engaged in a trade or commerce as defined by Section 501. 203(8), Florida Statutes.
3. Venue is proper in the Fifteenth Judicial Circuit as the statutory violations alleged herein occurred in or affected more than one judicial circuit in the State of Florida, while the Defendants’ principal places of business are located in Palm Beach County, Florida.

GENERAL ALLEGATIONS

I. PLAINTIFF

4. The Attorney General is an enforcing authority of FDUTPA and is authorized by Section 501.207(1)(b), Florida Statutes, to bring an action to enjoin any person who has violated, is violating, or is otherwise likely to violate FDUTPA, and by Section 501.207(3), Florida Statutes, to obtain further equitable relief, as appropriate.

5. The State of Florida has conducted an investigation, and the Attorney General has determined that an enforcement action serves the public interest, as required by Section 501.207(2), Florida Statutes.

II. LEAD DEFENDANT

6. Defendant GoReadyCalls Marketing, LLC, is a Florida Limited Liability Company organized under the laws of Florida on or about December 16, 2014, with the listed principal address currently being 12550 S. Military Trail, Boynton Beach, Florida 33436. Prior to March 25, 2016, the listed principal address was 14915 74th Street North, Loxahatchee, Florida 33470. At all times material to this Complaint, Evan Keen was the listed Registered Agent and Manager; and on or before April 26, 2015, Adam Lennox was added as an Authorized Member and Manager.

7. Since its inception, Lead Defendant has marketed, advertised, and sold products and services to consumers relating to technical support services for personal computers.

8. Lead Defendant is owned by two individuals, Adam Lennox and Evan Keen, that have operated an organization, comprised of several entities with various names, organized under the laws of Florida, and registered with the Florida Department of State, that share the same objective as Lead Defendant – to market, advertise, and sell products and services to consumers relating to technical support services for personal computers. In addition, these entities (defined above as the Enterprise Defendants) share owners, managers, business premises, and commingle funds.

III. ENTERPRISE DEFENDANTS

9. Kradanomic Solutions, LLC (“Kradanomic Solutions”) is a Florida Limited Liability Company organized under the laws of Florida on or about January 7, 2015. The currently listed principal address is 5837 Northpoint Ln, Boynton Beach, Florida 33437. Prior to March 9, 2016, the principal address was listed as 4268 Brandon Drive, Delray Beach, Florida 33445.

10. At all relevant times, Adam Lennox was the listed Registered Agent.
11. Kradanomic Solutions comingled funds with other Defendants.
12. Wizard Tech Solutions, LLC (“Wizard Tech Solutions”) is a Florida Limited Liability Company organized under the laws of Florida on or about March 16, 2015, with a principal address of 1615 S. Congress Avenue, Suite 103, Delray Beach, Florida 33445.
13. At all relevant times, Evan Keen was the listed Registered Agent and Authorized Member. At the time of the original filing, Michael Distefano was also a listed Authorized Member. On or before January 15, 2016, Distefano was removed and Adam Lennox was added as an Authorized Member.
14. The website for Wizard Tech Solutions, “wizardtech.support,” lists its address as 12550 S. Military Trail, Boynton Beach, FL 33436, and thus conducts business out of the same locations as other Defendants.
15. In addition, the homepage of wizardtech.support advertises tech support products and services, including the products, Defender Pro and TrackOFF. Individual Defendant Evan Keen is the listed registrant for the domain, wizardtech.support.
16. The content, design, and layout of websites for other Defendants is similar to the website for Wizard Tech Solutions. For example, both website homepages of “securedigitalit.com” and “wizardtech.support” contain the following quote and same contact telephone number: “In need of immediate assistance? Call us now! Our certified technicians are standing by to assist you!” The phone number listed on both sites is 888-812-7162. In addition, both websites advertise the same two products, Defender Pro and TrackOFF.
17. Wizard Tech Solutions comingled funds with other Defendants.

18. TeamKeen, LLC (“TeamKeen”) is a Florida Limited Liability Company, organized under the laws of Florida on or about December 21, 2015, with a listed principal address as 1653 NE 3rd Avenue, Delray Beach, Florida 33444.
19. At all relevant times, Evan Keen was the listed Registered Agent and listed Authorized Member. At all relevant times, Livia Rocha Da Silva was also a listed Authorized Member.
20. TeamKeen comingled funds with other Defendants and on some occasions, noted that the payments were for “Marketing,” “Advertising,” “Business Loan,” “Payroll,” and “Half of Profits For The Week.”
21. Cutting Edge Outlook, LLC (“Cutting Edge Outlook”) is a Florida Limited Liability Company, organized under the laws of Florida on or about December 24, 2015, with a listed principal address as 1300 NW 17th Avenue, Suite 260, Delray Beach, Florida 33445.
22. At all relevant times, Evan Keen was the listed Registered Agent and an Authorized Member. At all relevant times, Adam Lennox was also a listed Authorized Member.
23. Cutting Edge Outlook is also listed as an Authorized Member of US Software Pros LLC, another Enterprise Defendant, described below.
24. Cutting Edge Outlook conducts business at the same address as other Defendants.
25. Cutting Edge Outlook comingled funds with other Defendants and at times, noted that the payments were for “US Tech Marketing Pop Services,” “GoReadyCalls Marketing.” In addition, financial statements for Cutting Edge Outlook reflect several payments for the software, “TrackOFF.”
26. US Software Experts, LLC (“US Software Experts”) is a Florida Limited Liability Company, organized under the laws of Florida on or about January 25, 2016, with a listed principal address as 12550 S. Military Trail, Unit 8, Boynton Beach, Florida 33436.

27. US Software Experts conducts business at the same address as other Defendants.
28. At all relevant times, Adam Lennox was the listed Registered Agent and Manager.
29. Secure IT Digital Solutions, LLC (“Secure IT Digital Solutions”) is a Florida Limited Liability Company, organized under the laws of Florida on or about February 29, 2016, with a listed principal address as 1300 NW 17th Avenue, Delray Beach, Florida 33445.
30. Secure IT Digital Solutions conducts business at the same address as other Defendants.
31. Secure IT Digital Solutions comingles funds with other Defendants.
32. At all relevant times, Evan Keen was the listed Registered Agent and an Authorized Member. At all relevant times, Adam Lennox was also a listed Authorized Member.
33. Capital Investments LLC (“Capital Investments”) is a Florida Limited Liability Company, organized under the laws of Florida on or about March 10, 2016, with a listed principal address as 12550 S. Military Trail, Unit 8, Boynton Beach, Florida 33436.
34. At all relevant times, Evan Keen was the listed Registered Agent and an Authorized Member. At all relevant times, Adam Lennox was also a listed Authorized Member.
35. Capital Investments conducts business at the same address as other Defendants.
36. The website for Capital Investments, “capitalinvesting.net,” reflects that it conducts business at the same address as other Defendants. The homepage for this website provides that “Capital Investments is one of the leading players in the Internet domain market, working with investors to buy domain names at low costs, and selling them at maximum value.” Evan Keen is the listed registrant for the domain, “capitalinvesting.net.”
37. Capital Investments comingled funds with other Defendants, and made payments to the same third parties, paid by other Defendants.

38. A.E.A Worldwide, LLC (“A.E.A Worldwide”) is a Florida Limited Liability Company, organized under the laws of Florida on or about March 23, 2016, with a currently listed principal address of 21301 Powerline Rd, 106, Boca Raton, Florida 33433. Prior to January 11, 2017, the listed principal address was 12550 S. Military Trail, Unit 8, Boynton Beach, Florida 33436.

39. At all relevant times, GoReadyCalls Marketing was the listed Registered Agent and an Authorized Member of A.E.A Worldwide. At the time of the original filing, Ahren Sindelar was also a listed Authorized Member. On or before January 11, 2017, Sindelar was replaced by Matthew Schwartz as a listed Authorized Member.

40. A.E.A. Worldwide conducts business at the same location as other Defendants.

41. A.E.A. Worldwide commingles funds with other Defendants.

42. US Software Pros LLC (“US Software Pros”) was organized under the laws of Florida on or about August 30, 2016, with a listed principal address of 12550 S. Military Trail, Suite 6, Boynton Beach, Florida 33436.

43. At all relevant times, Andrew Gilbody was the listed Registered Agent, with Enterprise Defendant, Cutting Edge Outlook, as a listed Authorized Member.

44. US Software Pros conducts business at the same location as other Defendants.

45. The website for US Software Pros, “ussoftwarepros.com,” reflects that the location is at 12550 S. Military Trail, Boynton Beach, Florida 33436, which is the same location as other Defendants. The website also advertises similar software products as other Defendants, including Defender Pro, TrackOFF, and PC Medic. Adam Lennox is the listed registrant for the domain, “ussoftwarepros.com.”

46. US Software Pros commingles funds with other Defendants and has at times noted that the transfers of funds were for “Consulting,” “Marketing,” or “Advertising.”

47. Software Pros LLC (“Software Pros”) is a Florida Limited Liability Company, organized under the laws of Florida on March 14, 2017, with a listed principal address at 21301 Powerline Rd, #106, Boca Raton, Florida 33433. Since its inception, Derek J. Mauro and GoReadyCalls Marketing, LLC have been the listed Authorized Members.

48. Software Pros shares the same address as other Defendants and is owned by Lead Defendant.

49. The Enterprise Defendants have operated as a common enterprise with Lead Defendant while engaging in the deceptive acts and practices and other violations of law alleged below.

50. The Enterprise Defendants and Lead Defendant have common ownership, operations, and control; they conduct business out of the same principal locations, share managers, and commingle funds.

51. Because the Enterprise Defendants have operated as a common enterprise with Lead Defendant, each of them is jointly and severally liable for the acts and practices of the Lead Defendant.

52. The Enterprise Defendants have formulated, directed, controlled, had the authority to control, or participated in the acts and practices of the Lead Defendant that constitute the common enterprise.

IV. INDIVIDUAL DEFENDANTS

53. Defendant Adam Lennox is an owner, officer, director, member, or manager of the Common Enterprise.

54. 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 of the Common Enterprise, set forth in this Complaint.

55. For example, Adam Lennox is listed as a Registered Agent and/or Authorized Person on Defendant filings with the Department of State, Division of Corporations, including filings for: GoReadyCalls Marketing, Wizard Tech Solutions, Cutting Edge Outlook, Secure IT Digital Solutions, Capital Investments, Kradanomic Solutions, and US Software Experts.

56. Adam Lennox is the listed registrant for the website, “ussoftwarepros.com.”

57. Adam Lennox is an authorized signatory on several bank accounts for entities that constitute the Common Enterprise.

58. Further, communications between Adam Lennox, Evan Keen, Inbound Call Centers, and Networks, reflect his knowledge of the substance of the allegations below.

59. Defendant Adam Lennox resides at 4879 Lincoln Rd., Delray Beach, Florida 33445, is not in the military, and is otherwise *sui juris*.

60. Defendant Evan Keen is an owner, officer, director, member, or manager of the Common Enterprise.

61. 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 of the Common Enterprise, as set forth in this Complaint.

62. Specifically, Evan Keen is listed as a Registered Agent and/or Authorized Person on Defendant filings with the Department of State, Division of Corporations, including filings for: GoReadyCalls Marketing, Wizard Tech Solutions, Cutting Edge Outlook, Secure IT Digital Solutions, Capital Investments, and TeamKeen.

63. Evan Keen is the listed registrant for the domains, “goreadycalls.net,” “wizardtech.support,” “securedigitalit.com,” and “capitalinvesting.net.”

64. Evan Keen is an authorized signatory on several bank accounts for entities that make up the Common Enterprise.

65. Further, communications between Evan Keen, Adam Lennox, Inbound Call Centers, and Networks, reflect his knowledge of the substance of the allegations below.

66. Defendant Evan Keen resides at 14915 76th Road N., Loxahatchee, FL 33470, is not in the military, and is otherwise *sui juris*.

67. **Chart 1**, below, provides the shared owners of the corporate entities, constituting the common enterprise.

Managing/Authorized Member	Corporate Entity
Adam Lennox & Evan Keen	GoReadyCalls Marketing Wizard Tech Solutions Cutting Edge Outlook Secure IT Digital Solutions Capital Investments
Adam Lennox (without Evan Keen)	Kradanomic Solutions US Software Experts
Evan Keen (without Adam Lennox)	TeamKeen
GoReadyCalls Marketing	A.E.A Worldwide Software Pros
Cutting Edge Outlook	US Software Pros
Andrew Gilbody	US Software Pros

[Chart 1]

68. **Chart 2**, below, provides the shared locations of the corporate entities, constituting the common enterprise.

Address	Entity Associated via FL DOS/entity's website
12550 S Military Trail, Boynton Beach	A.E.A Worldwide Capital Investments Cutting Edge Outlook GoReadyCalls Marketing Secure IT Digital Solutions US Software Experts US Software Pros Wizard Tech Solutions
1300 NW 17th Ave, Delray Beach	Cutting Edge Outlook Secure IT Digital Solutions
1615 S Congress Ave, Delray Beach	GoReadyCalls Marketing Wizard Tech Solutions
1653 NE 3rd Ave, Delray Beach	TeamKeen Cutting Edge Outlook
21301 Powerline Rd, Boca Raton	A.E.A. Worldwide Software Pros

[Chart 2]

V. DEFINITIONS

69. For clarity, the following terms used in this Complaint are defined as follows:

- a. "Pop-Up" – A window that appears on a consumer's computer screen, while the consumer is browsing on the internet, containing content. Examples of Pop-Ups, and the content that such Pop-Ups contain, are illustrated in Images 2-6 of this Complaint.
- b. "Lead Generation" – The process by which inbound consumer telephone calls are generated via online marketing tools.
- c. "Pop Traffic" – Lead Generation through the online dissemination of Pop-Ups.
- d. "Pop Calls" – Consumer calls that are generated via a Pop-Up.

- e. “Inbound Call Center” – Call center, where sales agents answer inbound consumer calls in response to a Pop-Up.
- f. “Advertising Broker” – Person or entity that offers Lead Generation Services to Inbound Call Centers.
- g. “Publisher” – A person or entity that creates and disseminates Pop-Ups.
- h. “Network” – A person or entity that connects Advertising Brokers and Publishers to generate inbound consumer calls for Inbound Call Centers.
- i. “Pay-per-call Performance Marketplace” – online exchange used by Networks to connect Advertising Brokers and Publishers to generate inbound consumer calls.
- j. “Pay-per-call Marketing” – type of performance marketing where an Advertising Broker charges Inbound Call Centers a fixed sum per inbound consumer call in response to a Pop-Up.

**SPECIFIC ALLEGATIONS OF DEFENDANTS’ UNFAIR, DECEPTIVE,
AND UNCONSCIONABLE BUSINESS PRACTICES**

I. INTRODUCTION

70. Defendants operate a common enterprise, and more specifically, a tech support scam enterprise, registered with Florida’s Department of State, under various names. The object of Defendants’ operation is to exploit consumers’ fears about computer viruses, malware, hackers, and other security threats, in order to ultimately convince consumers to purchase unnecessary and costly technical support services and software products.

71. Defendants’ scam operation engages in deceptive Lead Generation—supplying Pop Traffic to Inbound Call Centers—as well as deceptive outbound calls to consumers, as alleged below.

II. LEAD GENERATION

72. First, Defendants are Advertising Brokers, providing Lead Generation services to Inbound Call Centers that sell tech support related services and/or products to consumers. Specifically, Defendants charge Inbound Call Centers per consumer call that is generated in response to a deceptive internet Pop-Up.

73. Defendants coordinate with Networks and Publishers, who create and disseminate Pop-Ups, through a Pay-Per-Call Performance Marketplace, which is an online platform connecting Publishers and Inbound Call Centers, or Brokers on their behalf.

74. The Pop-Ups that generate inbound consumer calls mislead consumers to believe that their computer is infected with malware or another security threat, and instructs the consumer to dial a toll-free telephone number for immediate tech support help.

75. Consumers who dial the telephone number provided in the deceptive Pop-Up are connected to a sales agent of an Inbound Call Center, who then exploits the consumer's misimpression from the Pop-Up to confirm that the consumer's computer is infected and in need of immediate repair.

76. Defendants regularly communicate via skype and email with agents of the Inbound Call Centers, Publishers, and Networks, to assess the Lead Generation's effectiveness in generating consumer sales.

77. Defendants charge Inbound Call Centers a negotiated sum certain for each consumer call generated via deceptive Pop-Up and deliver over 2000 consumer calls a day.

78. For example, Defendants provided Lead Generation services for an Inbound Call Center, called Client Experts Care, LLC. Specifically, Defendants provided Client Experts Care, LLC with inbound consumer calls resulting from Pop-Ups from October 2, 2015 through at least February 12, 2016.

79. Defendants charged Client Experts Care, LLC \$9.00 per inbound consumer call and were given a limit of 8,000 Pop Calls a week.

80. The Defendants accept payment from Inbound Call Centers in advance of services, and on a regular basis, based on the negotiated price per call and daily call limit. For example, Client Experts Care, LLC paid Defendants approximately \$70,000 per week for Pop Traffic.

81. The Inbound Call Centers and Defendants reconcile the payment amounts due, upon the exchange of information, in the form of call logs, that confirm the number of consumer calls routed to the Inbound Call Center.

82. Defendants work with multiple Inbound Call Centers in South Florida and elsewhere, routing consumer calls under designated campaign names.

83. Specifically, Defendants use pay-per-call online platforms to assign toll-free telephone numbers to the Pop Traffic supplied by a Publisher and/or Network, and designate the Pop Traffic under a campaign name.

84. The Pop Traffic under each campaign name, consists of Pop-Ups that display the assigned toll-free telephone number. Thus, consumers, dialing the displayed telephone number, are routed to an Inbound Call Center under the designated campaign name.

85. In addition, Defendants are provided with information about each inbound consumer call they generate—including, the call timestamp, campaign name, identification of the answering sales agent, disposition of the call, consumer's caller ID, assigned campaign toll-free telephone number, duration of the call between the sales agent and consumer, and an audio recording of the conversation between the consumer and the Inbound Call Center's sales agent—through the pay-per-call online platform.

86. Defendants regularly send records containing the above-described information to the Inbound Call Centers to justify payments and reconcile amounts owed, pursuant to the pay-per-call arrangement.

87. Additionally, the Defendants regularly received feedback from Inbound Call Centers regarding the effectiveness of the Pop Traffic in generating sales. For example, Client Experts Care, LLC often sent Defendants screen snapshots containing sales data. *See Image 1.*

The screenshot shows a web interface for sales data. At the top, there are date filters for 'Start Date' (2015, 11, 6) and 'End Date' (2015, 11, 10), with a 'Hit' button below. Below the filters is a table with the following data:

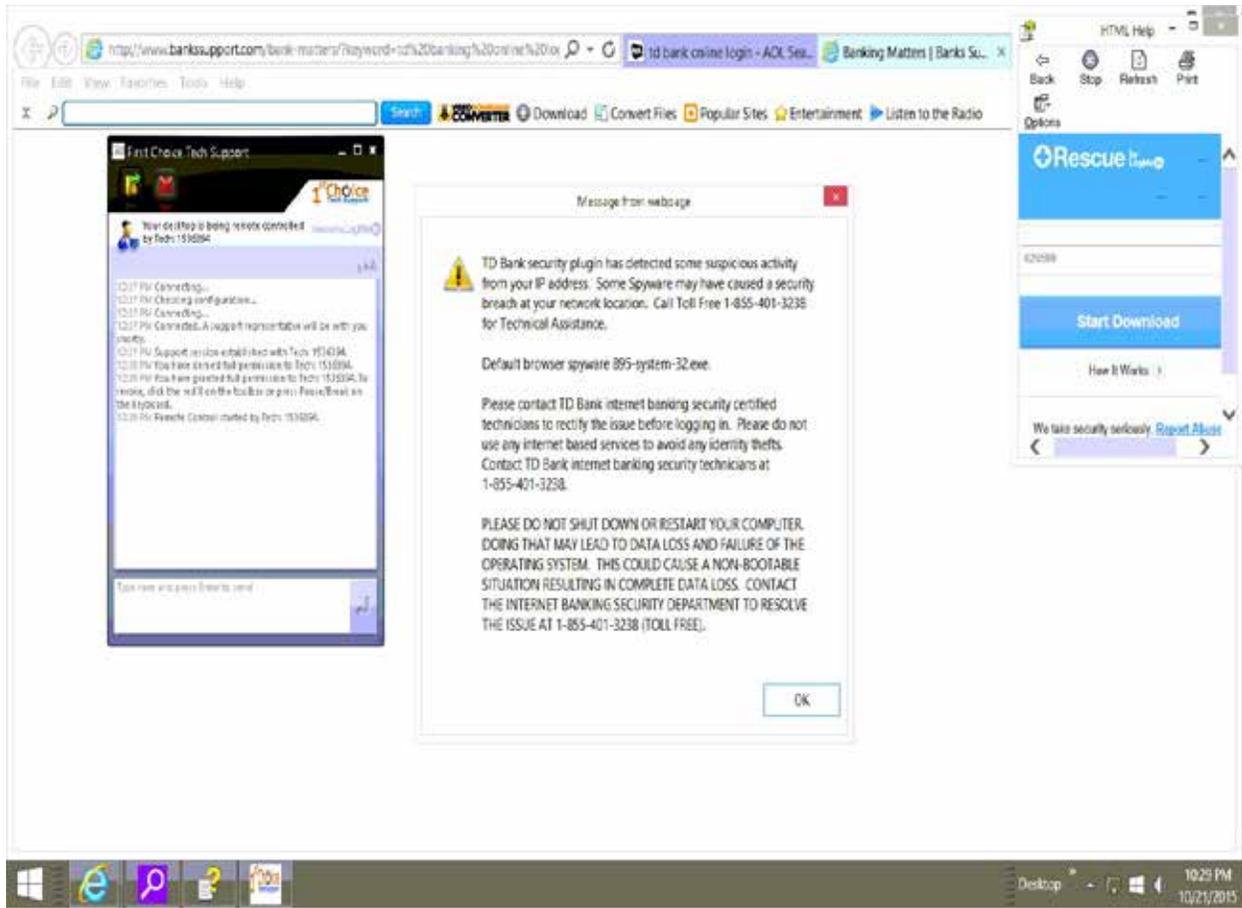
Campaign	Number of Calls (Raw)	Scrubbed Calls (30s)	Scrubbed Calls (60s)	Number of Sales	Conversion Rate	Conversion Rate (30s)	Conversion Rate (60s)	Total Sales Volume	Raw RPC	RPC (30s)	RPC (60s)
FOHTS COREADY 3	1164	1123	1065	Click to sort	13.33%	14.27%	14.33%	84539.96	72.71	75.00	76.00
FOHTS - inbound	664	654	642	108	16.26%	16.51%	16.32%	49300.00	74.24	75.38	76.79
FIRST CHOICE INBOUND	616	559	536	96	15.53%	17.17%	17.91%	44749.92	72.41	80.06	83.48
007 ZZ Tech - F5	1	1	1	0	0.00%	0.00%	0.00%	300.00	300.00	300.00	300.00

Unmatched Sales:

[Image 1]

88. Defendants have communicated with Inbound Call Centers, Publishers, and Networks regarding the deceptive content of the Pop-Ups.

89. One example of a deceptive Pop-Up Defendants utilized to drive inbound consumer calls to call centers is referred to as a “TD Bank Pop.” *See Image 2.*



[Image 2]

90. As shown above, TD Bank Pops serve to mislead reasonable consumers to believe that TD Bank sent the consumer a message, warning of a security breach. This Pop-Up provides that “TD Bank security plugin has detected some suspicious activity from your IP address. Some Spyware may have caused a security breach at your network location.” The Pop-Up provides a telephone number for the consumer to dial for help.

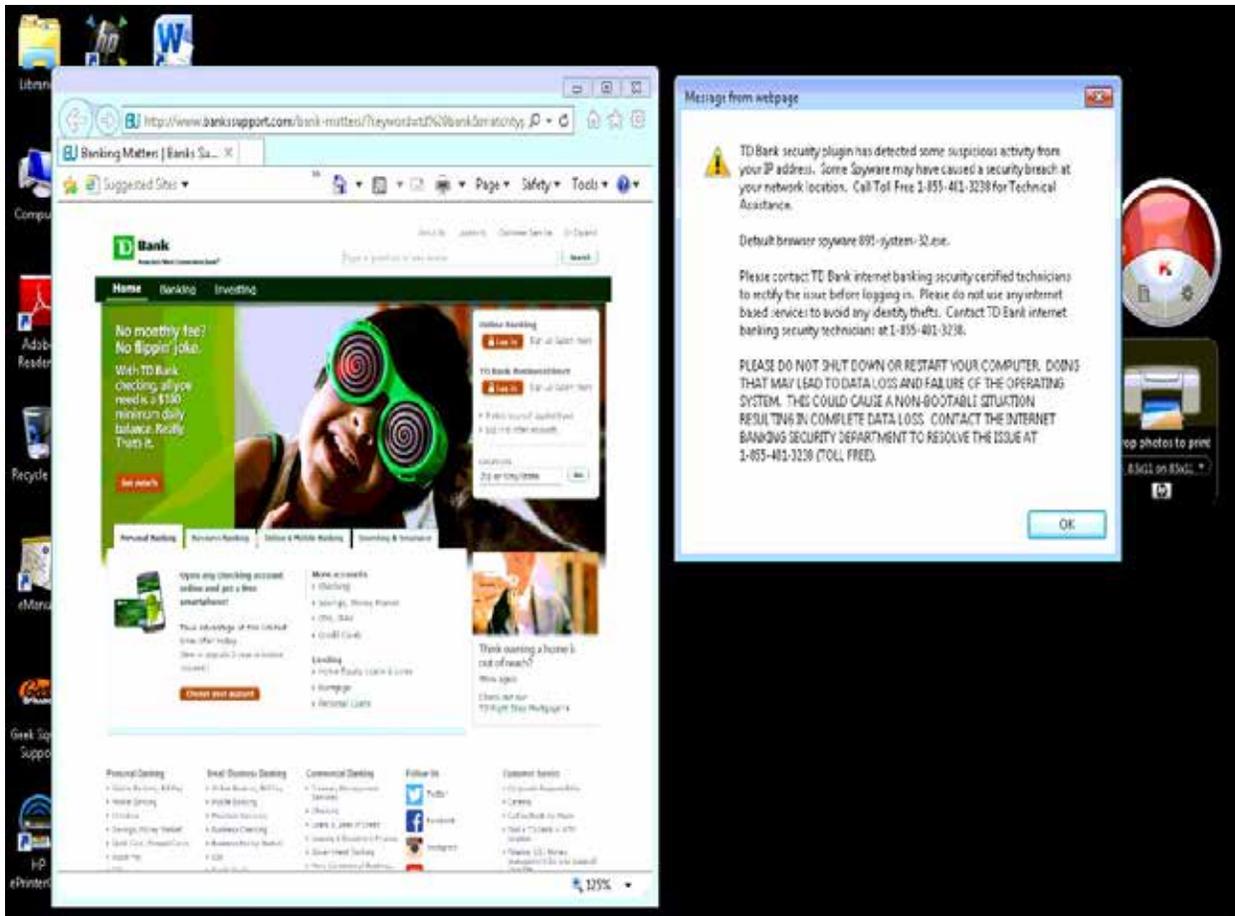
91. In addition, this Pop-Up states to the consumer, in summary, that using the internet could subject the consumer to identify theft, misleading the consumer to believe that a vulnerability has been detected by TD Bank, which is not true. Finally, this Pop-Up warns the consumer that any

action taken, other than dialing the telephone number, as directed, may lead to data loss and failure of the operating system.

92. Consumers have been subjected to the display of this Pop-Up while attempting to visit their bank website. A reasonable consumer would be misled to believe that this Pop-Up is a legitimate warning from their bank, and not simply an advertisement meant to lure them to contact an Inbound Call Center offering software services and/or products.

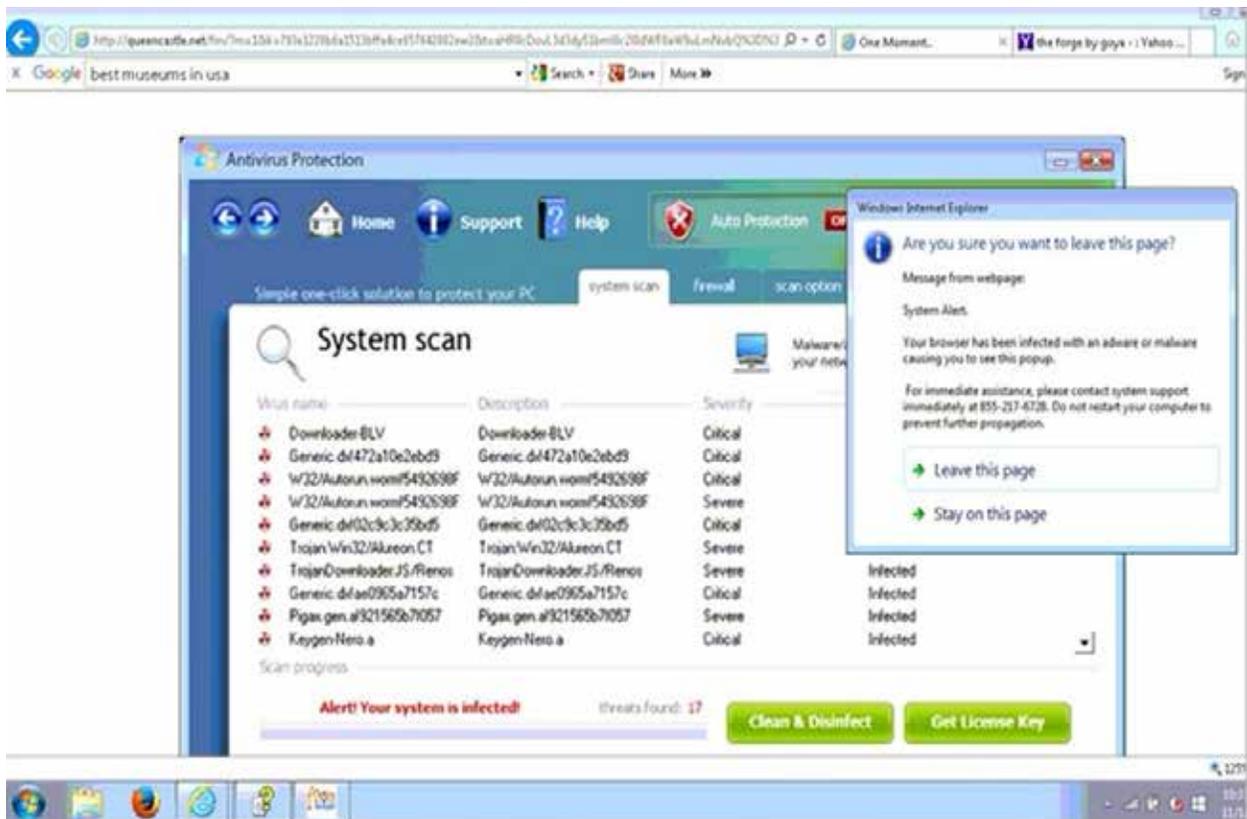
93. Defendants are aware that they have routed consumer calls to Inbound Call Centers caused by the display of TD Bank Pops. For example, Defendant Evan Keen admits in a communication with an Inbound Call Center, referencing TD Bank Pops, that “[a] lot of pubs are getting good results with that...”

94. In multiple instances, Defendants routed consumer calls to Inbound Call Centers, caused by the display of TD Bank Pops. *See Image 3* for example of a TD Bank Pop displayed in a different transaction.



[Image 3]

95. Another example of a deceptive Pop-Up utilized by Defendants to generate inbound consumer calls, is an internet window that purports to identify specific threats on the consumer’s computer and warns the consumer that their “browser has been infected with an adware or malware causing you to see this popup.” See **Image 4**.

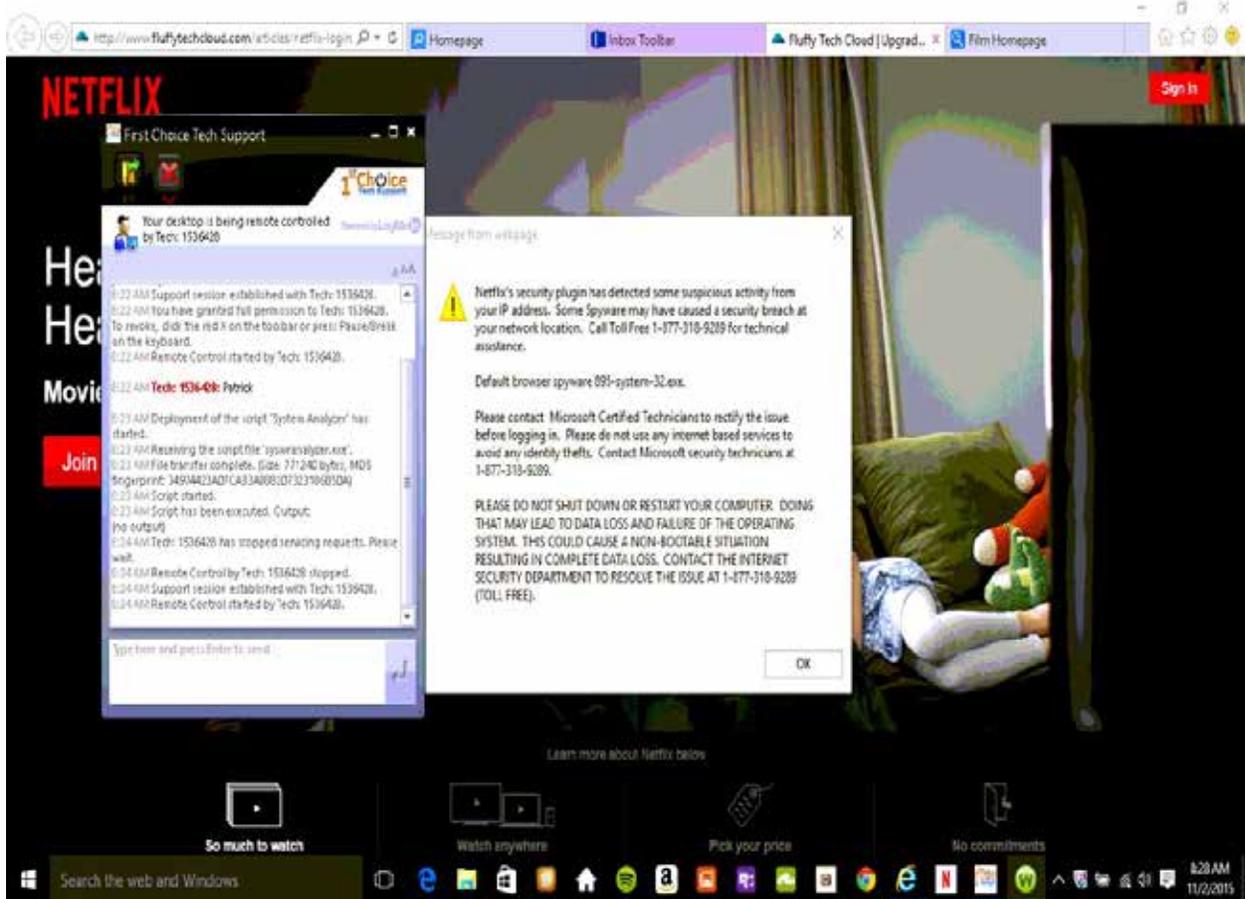


[Image 4]

96. Again, this Pop-Up would mislead a reasonable consumer to believe that their computer is infected with specific malware, as there is no indication that this Pop-Up is simply an advertisement meant to lure the consumer to contact an Inbound Call Center.

97. This Pop-Up also contains language that is meant to dissuade a consumer from clicking on the upper-right hand "X" to exit the window.

98. Defendants also utilize, what they refer to as, "Netflix Pops," to generate inbound consumer calls under the false premise that Netflix detected a security threat on the consumer's computer..." See **Image 5**.



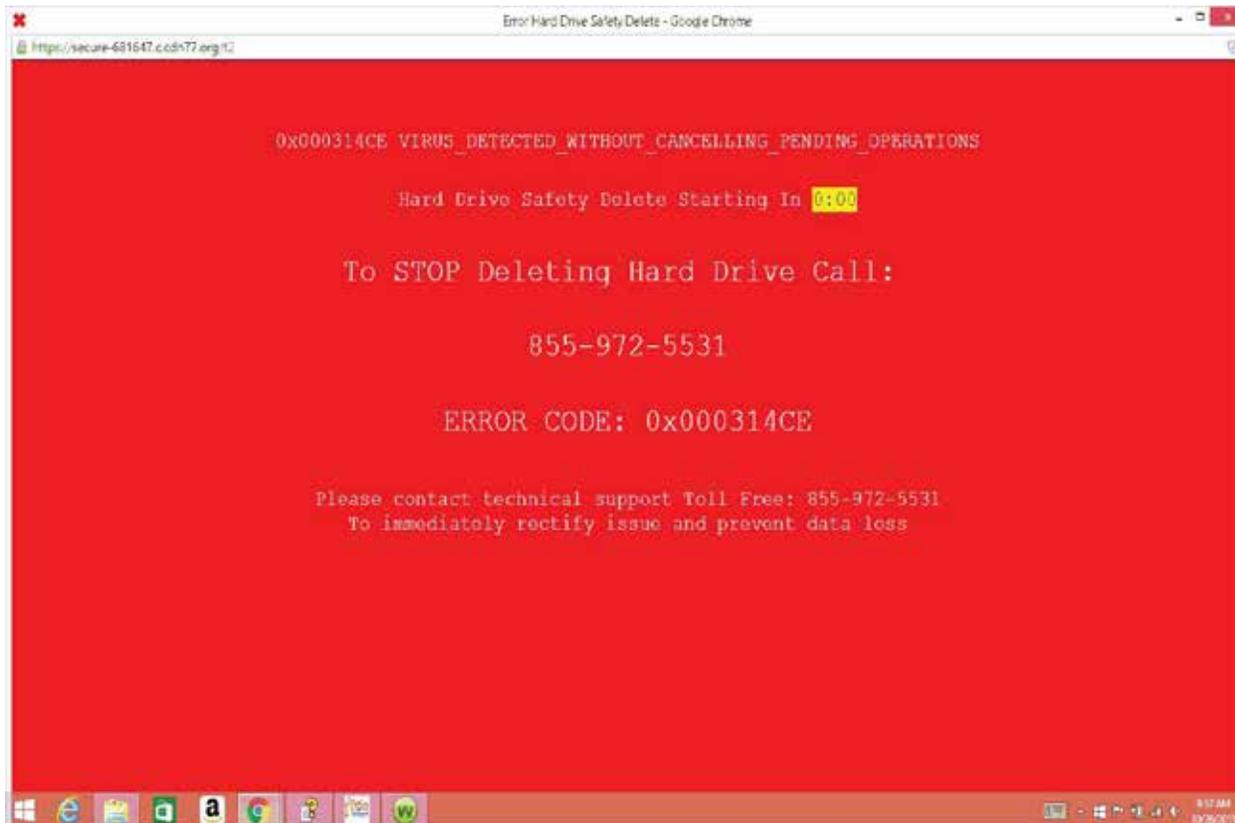
[Image 5]

99. The Netflix Pops warned consumers to:

NOT SHUT DOWN OR RESTART YOUR COMPUTER. DOING THAT MAY LEAD TO DATA LOSS AND FAILURE OF THE OPERATING SYSTEM. THIS COULD CAUSE A NON-BOOTABLE SITUATION RESULTING IN COMPLETE DATA LOSS. CONTACT THE INTERNET SECURITY DEPARTMENT TO RESOLVE THE ISSUE

100. Again, Netflix Pops contain content that would lead a reasonable consumer to believe that any action, other than dialing the toll-free telephone number, as directed, would further compromise the consumer's data. The Pop-Up content also misleads a reasonable consumer to believe that dialing the telephone number provided will connect them to Microsoft, which is false.

101. Another example of a deceptive and alarming Pop-Up utilized by Defendants to generate inbound consumer calls displays a count-down timer, and states that the consumer's hard drive will be deleted when the timer reaches 0.00. See **Image 6**.



[Image 6]

102. This Pop-Up creates a false sense of urgency, where consumers are misled to believe that they must dial the telephone number within a certain amount of time. There are several deceptive aspects of this Pop-Up, including a meaningless error code, and explicit language that would lead a reasonable consumer to believe that any action taken, other than dialing the telephone number as directed, will result in data loss.

103. Defendants use several variations of the above-described deceptive Pop-Ups to lure unsuspecting consumers to contact Inbound Call Centers, under the false premise that their computers are infected.

III. DEFENDANTS' CALL CENTER

104. Defendants also operate a call center, where Defendants' sales agents make outbound calls to consumers who previously fell victim to another tech support scam, in order to dupe them again into spending money on unnecessary and costly tech support services and/or products. Defendants use customer contact lists from tech support scams previously shut down by Court Order.

105. Specifically, Defendants' sales agents contact consumers, identifying themselves as "US Tech Support," and recite a sales script that purports to offer the consumer a complimentary diagnostic test to assure that the consumer's computer is running properly.

106. Defendants' sales script provides instructions so that the sales agent can gain remote access to the consumer's computer. Once the sales agent gains remote access to the consumer's computer, the sales agent recommends that the consumer upgrade their protection software if they already have such software, or recommends that they purchase protection software, if they do not already have such software.

107. Defendants' sales script also instructs sales agents to point out the number of processes running on a consumer's computer, and falsely states that Microsoft recommends that the processes should be between 30 and 50. Defendants' sales agents tell consumers that the high number of processes indicate that there is an issue on their computer, which is not true.

108. Defendants' sales agents also point out to consumers various innocuous graphics on the Event Viewer window and misrepresent that the consumer's computer contains several programs running in the background, making the computer "overwork itself."

109. To close the sale, Defendants' sales agents suggest to the consumer that they should take their computer to a local Office Max, Office Depot, or Staples to have a "level 3 technician" service their computer. Aside from the fact that there is no accepted industry designation of "level 3 technician," consumers are also falsely told that they will be charged around \$500 for a repair "like this" and will be without their computer for approximately 3-5 business days. Finally, consumers are told that if they take their computer to one of these stores, "in most cases you get the computer fixed and then this issue comes back within a month or two..."

110. Defendants' sales agents proceed to pitch to the consumer "Defender Pro," for \$300.00, "TrackOFF" for \$150.00, and "PC Medic Optimizer" for \$75.00.

111. At the conclusion of the scripted sales pitch, the consumer is told that they will see a charge on their credit card statement from Wizard Tech Support.

112. Defendants' scam enterprise has resulted in thousands of consumers worldwide purchasing tech support services and/or products under false pretenses, and has bilked consumers out of millions of dollars.

COUNT I
(Violation Of The Florida Deceptive And Unfair Trade Practices Act)

113. Plaintiff re-alleges paragraphs 1 through 112, as if set forth herein.

114. Section 501.204 of FDUTPA prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce."

115. As set forth in Paragraphs 1-112, which allegations are incorporated as if set forth herein, in numerous instances, in the course of marketing, offering for sale, and selling computer security and/or technical support services, the Defendants represent or have represented, expressly or by implication, through a variety of means, including through internet Pop-Ups and telephone calls,

that they have identified problems on consumers' computers that affect the performance or security of consumers' computers.

116. In truth and in fact, in numerous instances in which the Defendants have made the representations set forth in Paragraph 115, Defendants have not identified problems that affect the performance or security of consumers' computers.

117. The Defendants' representations as set forth in Paragraphs 1-112 of this Complaint are false and misleading and likely to mislead consumers acting reasonably, and/or consumers acting reasonably within the State of Florida.

118. Consumers were actually misled by the Defendants' misrepresentations in violation of Section 501.204 of FDUTPA.

119. The Enterprise Defendants have formulated, directed, controlled, had the authority to control, or participated in the acts and practices of the Lead Defendant that constitute the common enterprise.

120. The Individual Defendants, acting alone or in concert with others, formulated, directed, controlled, had the authority to control, or participated in the acts and practices of the Common Enterprise, as set forth in this Complaint.

121. Sections 501.207, 501.2075, and 501.2077, Florida Statutes, authorize this Court to grant such relief as this Court finds necessary to redress injury to consumers resulting from Defendants' violation of FDUTPA, including injunctive relief, the refund of monies paid, the disgorgement of ill-gotten monies, and civil penalties.

CONSUMER INJURY

122. Defendants' above-described acts and practices have injured and will likely continue to injure and prejudice the public and consumers in the State of Florida.

123. In addition, Defendants have been unjustly enriched as a result of their deceptive acts or practices.

124. Unless Defendants are permanently enjoined from engaging further in the acts and practices complained of herein, the continued activities of Defendants will result in irreparable injury to the public and to consumers in the State of Florida for which there is no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiff, Attorney General, pursuant to FDUTPA, requests that this Court:

- A. Order preliminary injunctive relief as to the Defendants in this Complaint, 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 FDUTPA by Defendants;
- C. Award such relief as the Court finds necessary to redress injury to consumers resulting from the Defendants' violations of the FDUTPA, including but not limited to, restitution to all consumers who are shown to have been injured, pursuant to Section 501.207, Florida Statutes; and such equitable or other relief as is just and appropriate

- pursuant to Section 501.207, Florida Statutes, including but not limited to, disgorgement of ill-gotten gains and repatriation of assets necessary to satisfy any judgment;
- D. Assess civil penalties in the amount of Ten Thousand Dollars (\$10,000.00) as prescribed by Section 501.2075, Florida Statutes, or Fifteen Thousand Dollars (\$15,000.00) for victimized senior citizens as prescribed by Section 501.2077, Florida Statutes; for each act or practice found to be in violation of FDUTPA;
 - E. Award attorneys' fees and costs pursuant to Section 501.2105, Florida Statutes or as otherwise authorized by law; and
 - F. Grant such other relief as this Court deems just and proper.

Dated this 28th day of April, 2017

Respectfully Submitted,

**PAMELA JO BONDI
ATTORNEY GENERAL**

/s/MichellePardoll
By: Michelle Pardoll
Assistant Attorney General
Florida Bar No. 0073915
Michelle.Pardoll@myfloridalegal.com
Office of the Attorney General
Consumer Protection Division
110 S.E. 6th Street, 10th Floor
Fort Lauderdale, Florida 33301
Telephone: (954) 712-4600

/s/ Genevieve Bonan
By: Genevieve Bonan

Assistant Attorney General
Florida Bar No. 109539
Genevieve.Bonan@myfloridalegal.com
Office of the Attorney General
1515 N. Flagler Dr., STE 900
West Palm Beach, Florida 33401
Telephone: (561) 837-5025