

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

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, *et al.*,

Defendants.

Case No. _____

[FILED UNDER SEAL]

RECEIVED

JUN 24 2016

THOMAS G BRUTON
CLERK, U S DISTRICT COURT

**MEMORANDUM IN SUPPORT OF PLAINTIFFS' *EX PARTE* MOTION FOR
TEMPORARY RESTRAINING ORDER WITH ASSET FREEZE, APPOINTMENT OF
A RECEIVER, OTHER EQUITABLE RELIEF, AND ORDER TO
SHOW CAUSE WHY A PRELIMINARY INJUNCTION SHOULD NOT ISSUE**

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Defendants’ Illegal Business Practices	3
	A. Defendants’ Deceptive Online Marketing	3
	B. The Sales Call	6
	1. Defendants Falsely Characterize Their Ads as Security Alerts	7
	2. Defendants’ Fraudulent Computer “Diagnostic”	8
	3. Defendants Falsely Claim to be Part of, or Certified by, Microsoft and Apple.....	15
	4. Closing the Sale	17
	C. Consumer Injury	20
III.	Defendants	20
	A. Florida Defendants.....	20
	B. Canadian Defendants	22
	C. Nevada Defendant.....	23
	D. Iowa Defendants	24
	E. Common Enterprise	24
IV.	Argument	25
	A. This Court Has the Authority to Grant the Requested Relief	25
	B. Plaintiffs Meet the Standard for Issuance of a Temporary Restraining Order	26
	1. Plaintiffs are Likely to Succeed on the Merits.....	27
	a. Deceptive Sales Practices in Violation of the FTC Act (Counts I and II).....	27
	b. Violations of the Telemarketing Sales Rule (Counts III and IV).....	29

c.	Violation of the Florida Deceptive and Unfair Trade Practices Act (Counts V and VI).....	30
2.	The Balance of Equities Strongly Favors Injunctive Relief	30
C.	The Individual Defendants are Liable for the Practices of the Corporate Defendants	31
D.	The Scope of the Proposed Temporary Restraining Order is Necessary and Appropriate	32
1.	Asset Freeze	32
2.	Temporary Receiver.....	33
3.	Immediate Access and Limited Expedited Discovery	33
E.	The Temporary Restraining Order Should Be Issued <i>Ex Parte</i>	34
V.	Conclusion	34

TABLE OF AUTHORITIES

Cases

Opinions

<i>Del. Watch v. FTC</i> , 332 F.2d 745 (2nd Cir. 1964)	31
<i>FTC v. Amy Travel Serv., Inc.</i> , 875 F.2d 564 (7th Cir. 1989)	25, 31
<i>FTC v. Bay Area Bus. Council, Inc.</i> , No. 02-cv-5762, 2003 WL 21003711 (N.D. Ill. May 1, 2003)	26
<i>FTC v. Bay Area Bus. Council, Inc.</i> , 423 F.3d 627 (7th Cir. 2005).....	27, 31
<i>FTC v. Cleverlink Trading Ltd.</i> , No. 05-cv-2889, 2006 WL 1735276 (N.D. Ill. June 19, 2006)	26
<i>FTC v. Datacom Mktg. Inc.</i> , No. 06-cv-2574, 2006 WL 1472644 (N.D. Ill. 2006).....	33
<i>FTC v. Direct Benefits Group, LLC</i> , 6:11-cv-1186-Orl-28TBS, 2013 WL 3771322 (M.D. Fla. July 18, 2013).....	31
<i>FTC v. Febre</i> , 128 F.3d 530 (7th Cir. 1997)	25
<i>FTC v. Figgie Int'l, Inc.</i> , 994 F.2d 595 (9th Cir. 1993).....	27, 28
<i>FTC v. Freecom Commc'ns, Inc.</i> , 401 F.3d 1192 (10th Cir. 2005).....	27
<i>FTC v. J.K. Publ'ns., Inc.</i> , 99 F. Supp. 2d 1176 (C.D. Cal. 2000)	31
<i>FTC v. Pantron I Corp.</i> , 33 F.3d 1088 (9th Cir. 1994).....	27
<i>FTC v. QT, Inc.</i> , 448 F. Supp. 2d 908 (N.D. Ill. 2006).....	27
<i>FTC v. Sabal</i> , 32 F. Supp. 2d 1004 (N.D. Ill. 1998).....	30
<i>FTC v. Sec. Rare Coin & Bullion Corp.</i> , 931 F.2d 1312 (8th Cir. 1991)	28
<i>FTC v. SlimAmerica, Inc.</i> , 77 F. Supp. 2d 1263 (S.D. Fla. 1999)	27
<i>FTC v. Stefanchik</i> , 559 F.3d 924 (9th Cir. 2009).....	27
<i>FTC v. Verity Int'l, Ltd.</i> , 443 F.3d 48 (2d Cir. 2006)	27
<i>FTC v. Wash. Data Res.</i> , 856 F. Supp. 2d 1247 (M.D. Fla. 2012)	24, 31

<i>FTC v. World Media Brokers</i> , 415 F.3d 758 (7th Cir. 2005)	27, 31
<i>FTC v. World Travel Vacation Brokers, Inc.</i> , 861 F.2d 1020 (7th Cir. 1988).....	25, 26, 30, 32, 33
<i>FTC v. World Wide Factors, Ltd.</i> , 882 F.2d 344 (9th Cir. 1989)	30
<i>Kraft, Inc. v. FTC</i> , 970 F.2d 311 (7th Cir. 1992).....	27

Orders and Filed Cases

<i>FTC v. 2145183 Ontario Inc., et al.</i> , No. 09-cv-7423 (N.D. Ill. Nov. 30, 2009)	32
<i>FTC v. Am. Tax Relief LLC, et al.</i> , No. 10-cv-6123 (N.D. Ill. Sept. 24, 2010).....	32
<i>FTC v. API Trade, LLC, et al.</i> , No. 10-cv-1543 (N.D. Ill. March 10, 2010).....	32
<i>FTC v. Apogee One Enterprises LLC et al.</i> , No. 12-cv-588 (N.D. Ill. Jan. 26, 2016).....	32
<i>FTC v. Asia Pacific Telecom, Inc., et al.</i> , No. 10-cv-3168 (N.D. Ill. May 25, 2010).....	32
<i>FTC v. Boost Software, Inc.</i> , No. 14-81397-CIV-MARRA (S.D. Fla. Nov. 12, 2014).....	2
<i>FTC v. Caprice Marketing LLC et al.</i> , No. 13-cv-6072 (N.D. Ill. Aug. 27, 2013).....	32
<i>FTC v. Click4Support, LLC</i> , No. 15-5777 (E.D. Pa. Oct. 10, 2015)	2
<i>FTC v. Finmaestros, LLC</i> , No.12-cv-7195-PAE (S.D.N.Y. Sept. 25, 2012)	2
<i>FTC v. Inbound Call Experts, LLC</i> , No. 14-81395-CIV-MARRA (S.D. Fla. Nov. 14, 2014).....	2
<i>FTC v. Lakshmi Infosoul Servs. Pvt. Ltd.</i> , No. 12-cv-7191-PAE (S.D.N.Y. Sept. 25, 2012)	2
<i>FTC v. Marczak</i> , No. 12-cv-7192-PAE (S.D.N.Y. Sept. 25, 2012).....	2
<i>FTC v. Pairsys, Inc.</i> , No. 14-cv-1192 (N.D.N.Y. Sept. 30, 2014).....	2
<i>FTC v. PCCare247 Inc.</i> , No. 1:12-cv-07189-PAE (S.D.N.Y. Sept. 25, 2012)	2
<i>FTC v. Pecon Software Ltd.</i> , No. 12-cv-7186-PAE (S.D.N.Y. Sept. 25, 2012).....	2
<i>FTC v. Stark Law, LLC et al.</i> , No. 16-cv-3463 (N.D. Ill. Mar. 26, 2016).....	32
<i>FTC v. Yellow Page Mktg., B.V., et al.</i> , No. 11-cv-05035 (N.D. Ill. July 26, 2011)	32
<i>State of Florida v. ASAP Tech Help, LLC</i> , No. 50-2015-CA002751 (Fla. 15 th Cir. Ct. 2015).....	2
<i>State of Florida v. E-Racer Tech, LLC</i> , No. 50-2015-CA-002753 (Fla. 15 th Cir. Ct. 2015).....	2

State of Florida v. ProTech Support, LLC, No. 50-2015-CA00278 (Fla. 15th Cir. Ct. 2015).....2

State of Florida v. TechFix USA, LLC, No. 50-2015-CA-002796 (Fla. 15th Cir. Ct. 2015).....2

Statutes

Federal Trade Commission Act, 15 U.S.C. § 45(a).....25, 30

15 U.S.C. § 53(b).....25, 26

The Florida Deceptive and Unfair Trade Practices Act,
Fla Stat. § 501.201 *et seq.*25, 30

Fla Stat. § 501.20425,30

Rules

Telemarketing Sales Rule, 16 C.F.R. Part 31025

16 C.F.R. § 310.3(a)(4).....29

16 C.F.R. § 310.2(dd)29

16 C.F.R. § 310.2 (ff).....29

16 C.F.R. § 310.2 (gg)29

Fed. R. Civ. P. 65(b)34

I. INTRODUCTION

The Federal Trade Commission and the State of Florida ask this Court to halt a technical support scam that exploits consumers' fears about viruses, malware, hackers, and other computer security threats. Doing business as Help Desk National, Defendants trick consumers into calling their telemarketing boiler room by using deceptive Internet ads that are designed to resemble security alerts from Microsoft or Apple, and that often prevent consumers' computers from functioning properly. These ads inform consumers that problems have been detected with their computers and urge them to call a toll-free number registered to Defendants for assistance. During calls with consumers, Defendants claim that they are certified by Microsoft and Apple to service computers running the Windows and OS X operating systems. These operating systems, Defendants explain, are programmed to display warnings when problems are detected ("like the check engine light on a car") and then direct users to call Help Desk National. After gaining remote access to consumers' computers, Defendants run a series of "diagnostic" tests and inevitably report to consumers that the tests have detected the existence of viruses, malware, hackers, or other threats. These problems, Defendants assert, present an immediate and grave threat to consumers' computers, as well as to the sensitive personal and financial data stored on them. Finally, after both frightening consumers and earning their trust, Defendants persuade them to spend hundreds of dollars for dubious "repairs" and security software.

Defendants' entire business is predicated on fraud. They are not certified or authorized by Microsoft or Apple to service products made by these companies. The alerts that lead consumers to call Defendants are advertisements, not warnings about actual problems with consumers' computers. These ads are part of an elaborate and highly deceptive ruse designed to

trick consumers into believing, without any basis, that their computers are in need of expensive repairs and software that only Defendants are capable of providing.

Over the past several years, complaints about technical support schemes like the one operated here by Defendants have increased exponentially. In 2015, for example, the FTC received nearly 40,000 complaints from consumers about this type of scam, a dramatic increase over the previous year.¹ In June 2016, moreover, the FBI's Internet Crime Complaint Center issued an alert regarding a recent spike in complaints about technical support scams, noting that it had received over 3600 complaints in the first four months of this year.² The FTC, Florida and other law enforcement agencies have responded to this alarming complaint growth by taking action against a series of companies engaged in conduct virtually identical to that here.³ Despite these actions, operations like Help Desk National have persisted with their deceptive schemes.

The FTC and Florida bring this motion *ex parte* to freeze Defendants' assets and immediately halt their fraudulent conduct, which has caused millions of dollars in consumer injury. The relief sought by Plaintiffs is supported by overwhelming evidence, including sworn statements from three of Defendants' former employees, eight consumers, a computer security expert, and representatives from Microsoft and Apple. Defendants' pattern of deceit, combined

¹ See "Consumer Sentinel Network Data Book for January – December 2015" at p. 82 (only 103 complaints in 2014) <<https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf>>.

² See "Public Service Announcement: Tech Support Scam," Alert Number I-060216-PSA <<https://www.ic3.gov/media/2016/160602.aspx>>.

³ See, e.g., *FTC v. Click4Support, LLC*, No. 15-5777 (E.D. Pa. Oct. 10, 2015); *State of Florida v. ASAP Tech Help, LLC*, No. 50-2015-CA002751 (Fla. 15th Cir. Ct. 2015); *State of Florida v. ProTech Support, LLC*, No. 50-2015-CA00278 (Fla. 15th Cir. Ct. 2015); *State of Florida v. E-Racer Tech, LLC*, No. 50-2015-CA-002753 (Fla. 15th Cir. Ct. 2015); *State of Florida v. TechFix USA, LLC*, No. 50-2015-CA-002796 (Fla. 15th Cir. Ct. 2015); *FTC v. Pairsys, Inc.*, No. 14-cv-1192 (N.D.N.Y. Sept. 30, 2014); *FTC v. Inbound Call Experts, LLC*, No. 14-81395-CIV-MARRA (S.D. Fla. Nov. 14, 2014); *FTC v. Boost Software, Inc.*, No. 14-81397-CIV-MARRA (S.D. Fla. Nov. 12, 2014); *FTC v. PCCare247 Inc.*, No. 1:12-cv-07189-PAE (S.D.N.Y. Sept. 25, 2012); *FTC v. Pecon Software Ltd.*, No. 12-cv-7186-PAE (S.D.N.Y. Sept. 25, 2012); *FTC v. Marczak*, No. 12-cv-7192-PAE (S.D.N.Y. Sept. 25, 2012); *FTC v. Finmaestros, LLC*, No. 12-cv-7195-PAE (S.D.N.Y. Sept. 25, 2012); *FTC v. Lakshmi Infosoul Servs. Pvt. Ltd.*, No. 12-cv-7191-PAE (S.D.N.Y. Sept. 25, 2012).

with their ongoing practice of transferring funds outside the country, suggest that they would hide or dissipate assets if they received notice of this action. The requested relief is necessary to preserve the Court's ability to provide effective final relief to Defendants' victims.

II. DEFENDANTS' ILLEGAL BUSINESS PRACTICES

A. Defendants' Deceptive Online Marketing

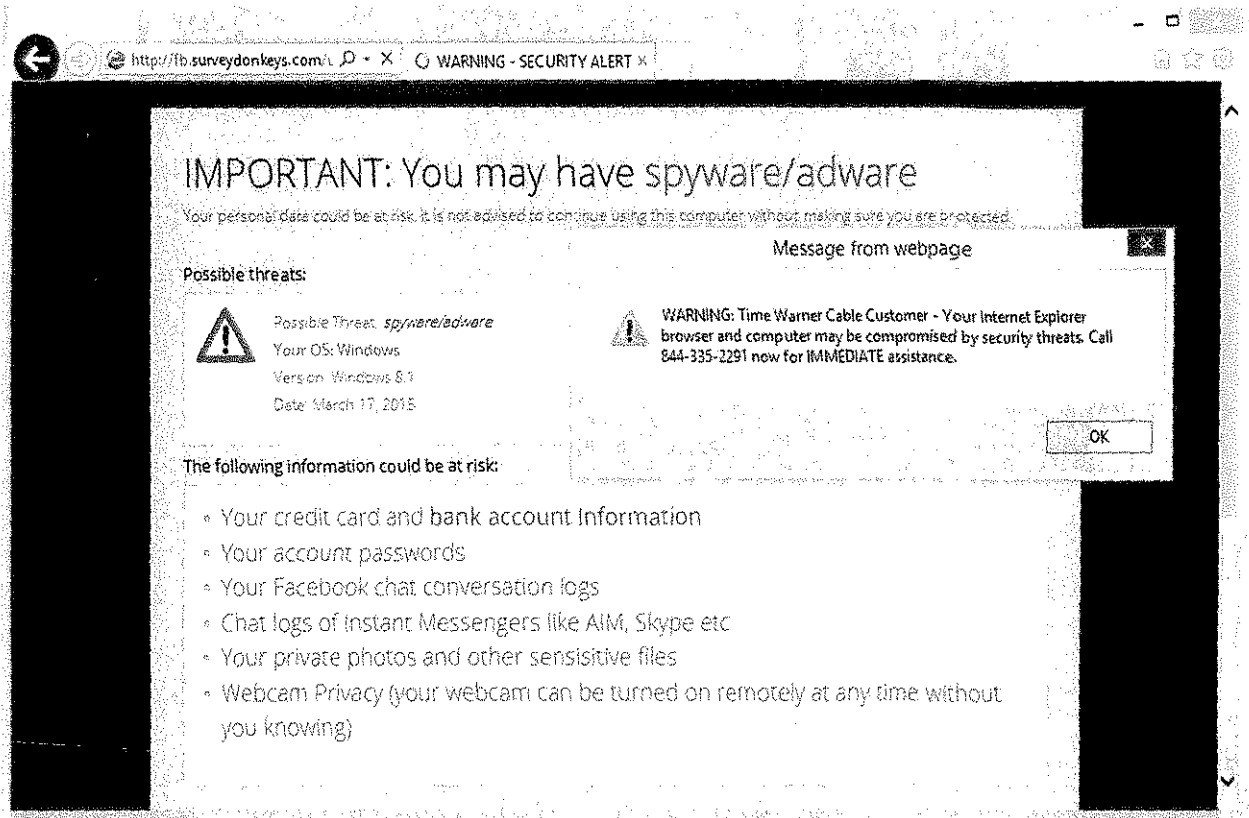
Consumers' first contact with this scheme is typically the sudden appearance on their computer screens of an Internet advertisement that takes one of two forms – a pop-up warning or a “chatbot.” In both cases, these ads mislead consumers into believing that there may be something seriously wrong with their computers and that calling a number displayed in the ad will put consumers into contact with a representative from Microsoft or Apple, or a technician certified by one of these companies. Defendants and their affiliate marketers cause consumers' computers to display these ads by a variety of means, including redirecting Internet traffic to websites programmed to display the pop-ups and chatbots.⁴

Defendants' pop-ups identify themselves as a “SECURITY ALERT” and are accompanied by warnings that consumers' computers may be infected with spyware that could place their “personal data” “at risk,” including bank account information, account passwords, and “other sensitive files.”⁵ A separate pop-up window advises consumers that their “Internet

⁴ PX 18, Declaration of Colin Page (“Page Dec.”) ¶ 16; PX 20, Declaration of Franklin Denton (“Denton Dec.”) ¶¶ 14-15; PX 11, Declaration of Lenny Zeltser (“Zeltser Dec.”) ¶¶ 4-5, 44-45.

⁵ PX 11, Zeltser Dec. ¶¶ 6-9, Att. B. Defendants' use of deceptive pop-up and chatbot advertisements is discussed in testimony provided by former employees, all of whom uniformly confirm that Defendants caused these ads to be displayed on consumers' computers and intentionally designed the ads to falsely resemble security alerts from Microsoft or Apple. *See* PX 18, Page Dec. ¶¶ 9-11; PX 19, Declaration of Giovanni Calaciura (“Calaciura Dec.”) ¶¶ 7-10; PX 20, Denton Dec. ¶¶ 12-18. This is, in fact, exactly how consumers perceived the ads. *See, e.g.*, PX 6, Declaration of Kent Brown (“Brown Dec.”) ¶ 5; PX 7, Declaration of Kathleen Law (“Law Dec.”) ¶¶ 5-6; PX 8, Declaration of Elizabeth Leahy (“Leahy Dec.”) ¶ 4 (“When my computer froze and I saw a message that said my computer was in trouble, especially a message that seemed to come from Microsoft, I panicked”); PX 10, Declaration of Margaret Salafrio (“Salafrio Dec.”) ¶ 4.

Explorer browser and computer may be compromised by security threats” and implores them to call a toll-free number “now for IMMEDIATE assistance.”⁶ A screenshot of one of Defendants’ pop-ups is below:⁷



The appearance of this pop-up is accompanied by a recorded voice reciting the following warning to consumers:

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.⁸

In many instances, Defendants’ pop-ups prevent consumers’ Internet browsers from functioning properly. Specifically, consumers are often unable to close the pop-ups and prevent new ones

⁶ PX 11, Zeltser Dec. Att. B.

⁷ *Id.*

⁸ *Id.* ¶ 12.

from appearing in their place.⁹ According to a former employee, Defendants make their pop-ups difficult to close in order to increase sales.¹⁰

Defendants also generate leads through the use of a so-called “chatbot.” A chatbot is a computer program that simulates human conversation over the Internet.¹¹ Defendants’ chatbots are designed to trick consumers into believing that they are communicating with a representative from Microsoft or Apple, or someone certified to service products made by these companies.¹² For example, Defendants’ chatbot windows often depict a man or woman identified as a “Microsoft Certified Partner,” who appears to ask questions and respond to input from consumers.¹³ The chatbot warns consumers that their computers are compromised in some way and “strongly urges” them to immediately call a toll-free number to speak with “one of our Microsoft Certified Partners to fix your computer problems.”¹⁴ This warning is accompanied by

⁹ When a user attempts to close the pop-up window, coding embedded in the webpage causes a new window to appear. *See, e.g., id.* ¶ 11; PX 4, Declaration of Denise Amos (“Amos Dec.”) ¶ 4; PX 5, Declaration of Richard Best (“Best Dec.”) ¶¶ 5, 9. In some instances, consumers are unable to remove these messages from their computers. *See, e.g.,* PX 1, Declaration of FTC Investigator Roberto Menjivar (“Menjivar Dec.”) ¶ 31, Att. Z at p. 2 (despite rebooting and powering down his computer several times, consumer could not make pop-ups go away). These are hallmarks of a form of malware known as a “browser hijacker,” which modifies the settings of a web browser without the user’s permission in order to display unwanted advertising. *See* “Browser Hijacking.” Wikipedia: The Free Encyclopedia. May 15, 2016. <https://en.wikipedia.org/wiki/Browser_hijacking>.

¹⁰ *See* PX 18, Page Dec. ¶ 12 (to increase revenue, Defendants would make their pop-ups more difficult to close); PX 19, Calaciura Dec. ¶ 8 (these more aggressive pop-ups are known as a “lock pops,” according to a former supervisor).

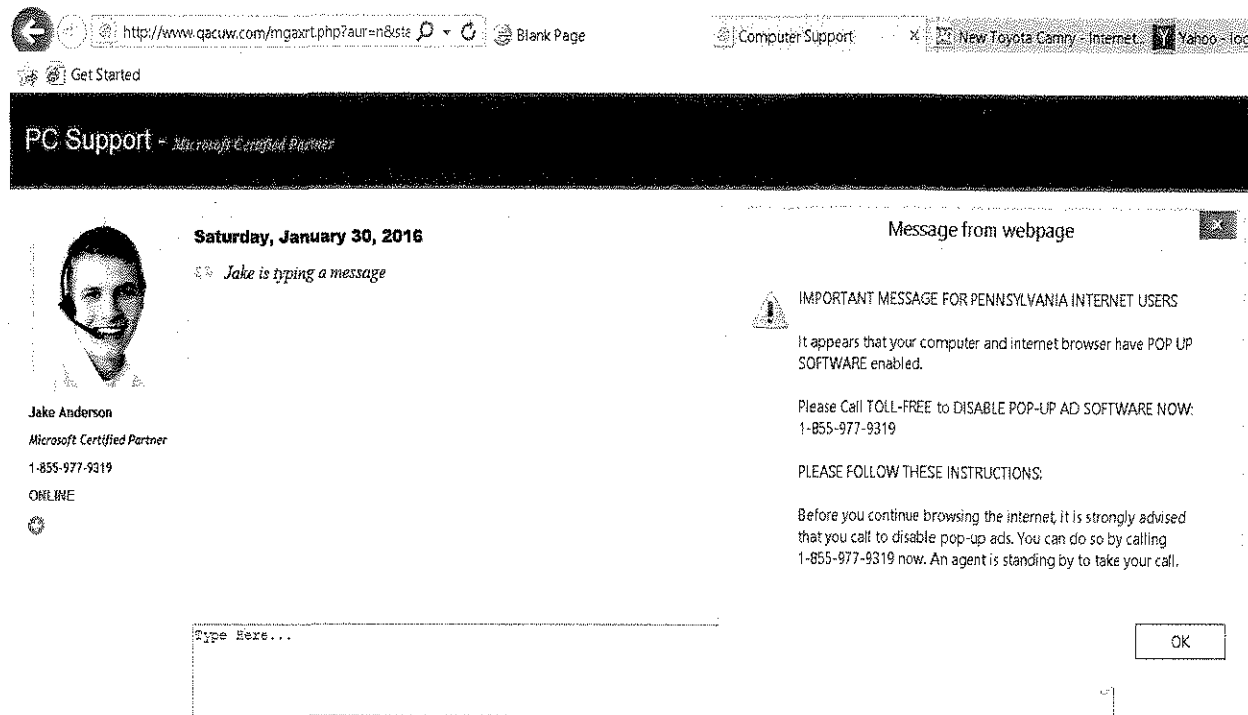
¹¹ *See* “Chatterbot.” Wikipedia: The Free Encyclopedia. June 1, 2016. <<https://en.wikipedia.org/wiki/Chatterbot>>.

¹² *See* declarations from Defendants’ former employees: PX 18, Page Dec. ¶ 11 (sales representative); PX 19, Calaciura Dec. ¶ 8 (supervisor); PX 20, Denton Dec. ¶ 13 (customer service representative).

¹³ Plaintiffs have identified three different chatbot personas used by Defendants: Jake Anderson, Gregg Foster, and Molly Jefferson. Each has its own profile picture. *See* PX 1, Menjivar Dec. ¶¶ 27-28, Atts. Q-S; PX 12, Declaration of FBI Special Agent Jennifer McGrath (“McGrath Dec.”) ¶¶ 4-5, Att. A.

¹⁴ *Id.*

a pop-up, which again instructs consumers to call the same number “NOW.”¹⁵ A screenshot of one of Defendants’ chatbots is below:¹⁶



B. The Sales Call

Defendants’ pop-up and chatbot ads all display a toll-free number registered to Defendants and urge consumers to call this number.¹⁷ Consumers who do so are connected to a telemarketer working at Defendants’ boiler room in Boynton Beach, Florida.¹⁸ Posing as Microsoft- and Apple-certified technicians, the telemarketers walk consumers through a high-

¹⁵ *Id.*

¹⁶ PX 12, McGrath Dec. Att. A; *see also* PX 1, Menjivar Dec., Atts. Q, R.

¹⁷ PX 1, Menjivar Dec. ¶¶ 10, 15-18 (summary of toll-free numbers assigned to Defendants by two telecommunications carriers as well as call records associated with these numbers).

¹⁸ *See* description of undercover calls made by FTC investigator, *id.* ¶¶ 32-54, and testimony of former employees, all of whom confirm that Defendants operate a call center in Boynton Beach, Florida that receives inbound calls generated by Defendants’ pop-up and chatbot ads. PX 18, Page Dec. ¶¶ 2, 8-9; PX 19, Calaciura Dec. ¶¶ 3, 7-8; PX 20, Denton Dec. ¶ 3.

pressure sales pitch disguised as a “diagnostic” test that always leads to the same conclusion – namely, that consumers need to pay hundreds of dollars to Defendants to address dubious problems supposedly identified by the test.

1. Defendants Falsely Characterize Their Ads as Security Alerts

Help Desk National telemarketers follow a written script that presupposes all incoming calls are a response to Defendants’ deceptive pop-up warnings and chatbots.¹⁹ This script directs telemarketers to begin their sales pitch by asking what “the message” says and then to mislead consumers into believing that these advertisements are actually security alerts from Microsoft, Apple, or their computer operating systems (“like the check engine light” on a car).²⁰ For example, the script falsely describes Defendants’ pop-ups and chatbots as “valuable tools to assess any risk or problems associated with your operating system.”²¹

Telemarketers often add their own embellishments to Defendants’ script. In an undercover call with an FTC investigator, a Help Desk National telemarketer characterized the appearance of a chatbot as “actually not good,” explaining that it “validates that something is wrong with your computer.”²² The same telemarketer later said that the chatbot “was the system notification telling you that’s something wrong with your system.”²³ Similarly, during a second undercover call, a telemarketer stated that the “only way” a chatbot “would show up on a computer is if a user recently downloaded some kind of an infection.”²⁴ Help Desk National

¹⁹ PX 1, Menjivar Dec. ¶ 30, Att. T (“Help Desk National Tech Support Script” and “Rebuttals”); PX 18, Page Dec. ¶ 3, 8, Att. A (same); PX 19, Calaciura Dec. ¶ 4, Att. A (same); PX 20, Denton Dec. ¶¶ 20, 22 (former customer service representative importance of Defendants’ script, which “always concluded with a diagnosis of severe computer issues”).

²⁰ See, e.g., PX 1, Menjivar Dec. Att. T at p. 1.

²¹ *Id.*

²² *Id.* Att. FF at p. 6.

²³ *Id.* at p. 23.

²⁴ *Id.* Att. GG at p. 5.

telemarketers regularly use these types of fabrications.²⁵ In many instances, telemarketers assert that the mere existence of a pop-up or chatbot on a consumer's computer is conclusive proof that the computer is infected and in need of Defendants' repair services.²⁶

Defendants' pop-ups and chatbots actually are advertisements that serve only one purpose – luring consumers into believing that there is something wrong with their computers so that they will then contact Defendants' call center. These advertisements do not diagnose problems with consumers' computers and are not capable of doing so.²⁷

2. Defendants' Fraudulent Computer "Diagnostic"

After convincing consumers that their computers may be severely compromised and in need of immediate repair, Defendants' telemarketers offer to provide a free "diagnostic." To do so, telemarketers explain, they must first gain remote access to consumers' computers. Remote

²⁵ See, e.g., PX 5, Best Dec. ¶ 7 (telemarketer claimed to know that consumer's computer was compromised prior to examining it because "Microsoft has embedded this pop-up response into the operating system to alert Help Desk National"); PX 10, Salafrio Dec. ¶ 5 (after consumer described appearance of chatbot on her computer, telemarketer claimed that computer was infected with a "browser hijacker" and "needed to be repaired immediately"); PX 11, Zeltser Dec. ¶ 16 (telemarketer claimed that pop-up ad is "actually a security feature that's built into the operating system"); PX 1, Menjivar Dec. Att. V at p. 2 ("This is your computer sensing that there's been an intrusion or some malicious software installed, and that's why it's directing you to call an Apple-certified technician"); *id.* Att. W at p. 2 ("So, you had an infection. [Your computer is] telling you to contact Microsoft-certified technicians at the Help Desk"); *id.* Att X at 3 (referring to a chatbot, a representative asked: "...do you have one of our Microsoft online solution providers there, Jake or Molly, somebody that was typing to you?").

²⁶ In these instances, telemarketers often skip the "diagnostic" described below and immediately begin pressuring callers into purchasing repair services and security software. See, e.g., PX 4, Amos Dec. ¶ 5; PX 8, Leahy Dec. ¶ 5; PX 10, Salafrio Dec. ¶ 5 (based solely on existence of chatbot, telemarketer declared that consumer's computer had a "browser hijacker" that would cost several hundred dollars to remove).

²⁷ Microsoft and Apple have each provided declarations stating unequivocally that their Windows and OS X computer operating systems do not include a feature designed to notify users of suspected performance or security problems through the use of pop-up messages. See PX 13, Declaration of Eric Barkve, Support Engineering Manager – OS Platforms, Apple Inc. ("Barkve Dec.") ¶¶ 4-5 (OS X operating system does not include a feature); PX 15, Declaration of Shawn Aebi, Service Delivery Manager for Consumer Services, Customer Service and Support, Microsoft Corporation ("Aebi Dec.") ¶ 10 (same testimony regarding Windows operating system). Similarly, neither company notifies users about suspected performance or security problems through the use of chatbots or authorizes third parties to do so. See PX 13, Barkve Dec. ¶ 5; PX 15, Aebi Dec. ¶ 10.

access gives telemarketers control over the computers, enabling them to move cursors, enter commands, run applications, and access stored information.²⁸

Once in control of consumers' computers, telemarketers run what they claim are a series of diagnostic tests, which are highly similar to the "diagnostics" performed by defendants named in law enforcement brought actions against other tech support scams.²⁹ Specifically, Help Desk National telemarketers with no formal technical training or expertise misrepresent the meaning of information displayed in applications built into the Windows and OS X operating systems to "diagnose" problems with consumers' computers.³⁰ Defendants also install a software program purportedly capable of assessing a computer's "overall health." In reality, these "tests" are not intended to diagnose actual problems, but are instead part of Defendants' sales pitch. Regardless of a computer's actual condition, Help Desk National telemarketers inevitably find reasons why consumers must spend hundreds of dollars to repair and protect their computers.³¹

²⁸ See PX 18, Page Dec. ¶¶ 18-19; PX 20, Denton Dec. ¶ 16; PX 19, Calaciura Dec. ¶¶ 11-12. Defendants remotely access consumers' computers using a service provided by LogMeIn, a technology company. See PX 1, Menjivar Dec. ¶ 19.

²⁹ See PX 18, Page Dec. ¶ 4 (according to former employee, Defendants' practices similar to those engaged in by another technical support scam sued by Plaintiffs, probably even worse); PX 20, Denton Dec. ¶ 4 (Defendants' "employed the same business model" as two other technical support scams subject to previous enforcement actions); PX 17, Declaration of Jeffrey McJunkin ("McJunkin Dec.") Dec. ¶¶ 3-4 (similarities between Defendants' "diagnostic" evaluations and tactics used by two other technical support scams sued by Plaintiffs).

³⁰ These "diagnostic" evaluations, as well as the lack of qualifications of those hired to perform and interpret them, are described by former employees. See PX 18, Page Dec. ¶¶ 4, 20, 23 ("When I asked one technician how she obtained her position, she said that she had simply requested a transfer from sales" and that her "computer expertise consisted of on-the-job training"); PX 19, Calaciura Dec. ¶¶ 14-18; PX 20, Denton Dec. ¶¶ 4, 22. As outlined in Defendants' sales script, after obtaining remote access to a consumer's computer, Defendants usually open the Microsoft Task Manager and System Configuration utility. See PX 1, Menjivar Dec. Att. T at pp. 3-4; PX 18, Page Dec. Att. A at 3-5; PX 19, Calaciura Dec. Att. A at pp. 2-3. The process for Apple computers is also detailed in these scripts. See PX 1, Menjivar Dec., Att. T at pp. 3-4 ("Mac Script").

³¹ The deterministic nature of this process is attested to by Defendants' former employees, who state that they were always expected to invent some justification for alleging that a computer showed signs of performance or security problems. See PX 18, Page Dec. ¶ 20; PX 19, Calaciura Dec. ¶¶ 14-18; PX 20, Denton Dec. ¶ 22. It is also evident in Defendants script, as well as the three undercover calls conducted by the FTC and Lenny Zeltser, discussed below, all of which involved the use of pristine

The utterly fraudulent nature of Help Desk National's diagnostic evaluations is exemplified best by undercover purchases conducted by the FTC and independent computer security expert, Lenny Zeltser, each posing as consumers.³² Both the FTC investigator and Zeltser each used computers running a clean version of the Windows operating system free of any malicious programs or other threats.³³ Nevertheless, in each case, Help Desk National telemarketers claimed to discover unmistakable evidence of severe problems that only a Microsoft-certified technician could fix. For example, the telemarketer examining Zeltser's computer erroneously claimed it was running too many "processes" and that this explained the appearance of the pop-up advertisement directing Zeltser to call Help Desk National.³⁴ In reality, Zeltser had allowed the telemarketer to remotely access a computer that Zeltser maintains in a laboratory setting in "pristine condition."³⁵ The telemarketer charged Zeltser \$250 to

computers that were nevertheless found to be in need of urgent repairs costing hundreds of dollars. PX 17, McJunkin Dec. ¶¶ 7-9.

³² The FTC conducted two separate undercover calls as part of its investigation of Defendants' business practices. FTC investigator Roberto Menjivar initiated these calls on May 10, 2016 at approximately 4:23 p.m. Eastern time ("Call One") and May 11, 2016 at approximately 12:52 p.m. Eastern time ("Call Two"). PX 1, Menjivar Dec. ¶¶ 40, 48. During these calls, Mr. Menjivar posed as a consumer and FTC staff recorded his conversations with Defendants as well as related computer activity during the remote access sessions. *Id.* ¶¶ 36-39. In addition, computer security expert Lenny Zeltser independently conducted his own undercover purchase on March 17, 2015, and subsequently documented this experience in a blog that he maintains. Plaintiffs have obtained a declaration from Mr. Zeltser. *See* PX 11, Zeltser Dec.

³³ Tina Del Beccaro, an information technology specialist employed by the FTC, set up the computer used to conduct Plaintiffs' undercover calls. *See* PX 3, Declaration of Tina Del Beccaro. Before each call, Ms. Del Beccaro installed a clean version of Microsoft Windows 7 Professional and arranged for a second computer to capture screen images and Internet traffic on the undercover machine. *Id.* ¶¶ 6-14. Calvin Brown, an FTC forensic examiner, created pre- and post-call forensic images of the hard drive used for each purchase. *See* PX 2, Declaration of Calvin Brown. Mr. Brown then provided copies of these hard drive images to Jeff McJunkin, a computer forensics and security expert retained by Plaintiffs. *Id.* ¶ 14. Mr. McJunkin examined these hard drive images and found that they showed no signs of malware, including viruses, spyware, adware, worms, scareware, or any other malicious code or activity before the calls. *See* PX 17, McJunkin Dec. ¶¶ 7-9.

³⁴ PX 11, Zeltser Dec. ¶¶ 19, 28-31.

³⁵ *Id.* ¶¶ 10, 32 ("I am confident that my computer was not compromised or at any particular heightened risk. I operate my computer in a secure laboratory environment, and keep it isolated from the Internet except when I am using it to investigate malware or other technology issues... This computer is set up as a virtualized system in pristine condition.")

“repair” non-existent problems on Zeltser’s computer and install an antimalware program known as STOPZilla, which the telemarketer falsely described as a “Microsoft Silver product.”³⁶

Help Desk National telemarketers who spoke to the FTC’s investigator offered even flimsier justifications to support their recommended “repairs.” During the first call, after gaining remote access to a clean FTC computer, Defendants’ telemarketer, who identified himself as “Derek,” installed and ran a third-party application known as Webroot System Analyzer (“Webroot”).³⁷ Results of the Webroot scan, according to Derek, showed “an infection in the system...coming from overseas,” which, if not removed, would “try to compromise account numbers, routing numbers, usernames, passwords, debit card information or credit card information.”³⁸ Derek also warned that the virus “could potentially destabilize your whole entire operating system to where the damage would be irreplaceable and your machine would be completely shot.”³⁹ Saying that he wanted to “check one other thing real quick,” Derek then opened the following window in Webroot.⁴⁰

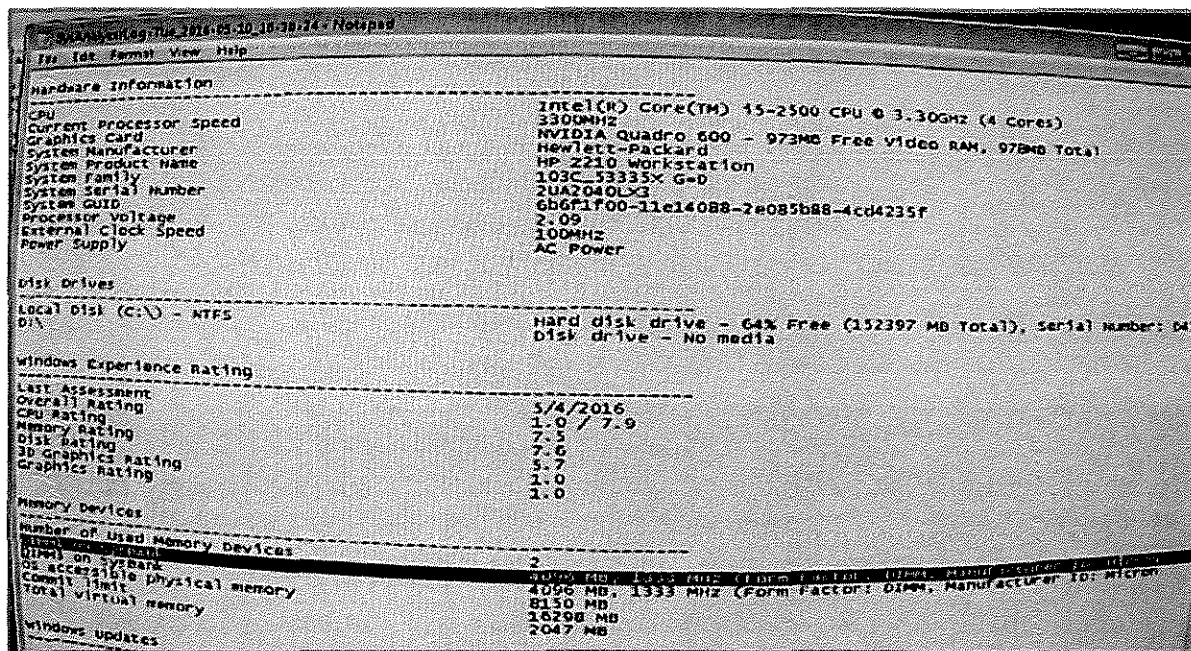
³⁶ *Id.* ¶¶ 22-26.

³⁷ PX 1, Menjivar Dec. ¶ 40-43, 60.

³⁸ *Id.* Att. FF at p. 21.

³⁹ *Id.*

⁴⁰ PX 17, McJunkin Dec. ¶ 18.



Derek scrolled down to a section labeled “Memory Devices” and immediately highlighted two rows, as shown in the image above.⁴¹ Referring to the highlighted text “SysBank” and “4096,” Derek ominously declared that the banking information on the computer was at risk: “Look at this. That – your banking information is tied into the system in almost 4,100 areas with a virus that scans, analyzes and monitors the machine.”⁴² Shortly thereafter, Derek opened a separate window and directed the investigator to input his credit card information to pay the \$250 fee for removal of this “infection.”⁴³

During the second undercover call, a Help Desk National telemarketer named “Jake” obtained remote access to another clean FTC computer, opened the Windows System Configuration utility, selected the “startup” tab, and directed the investigator’s attention to a

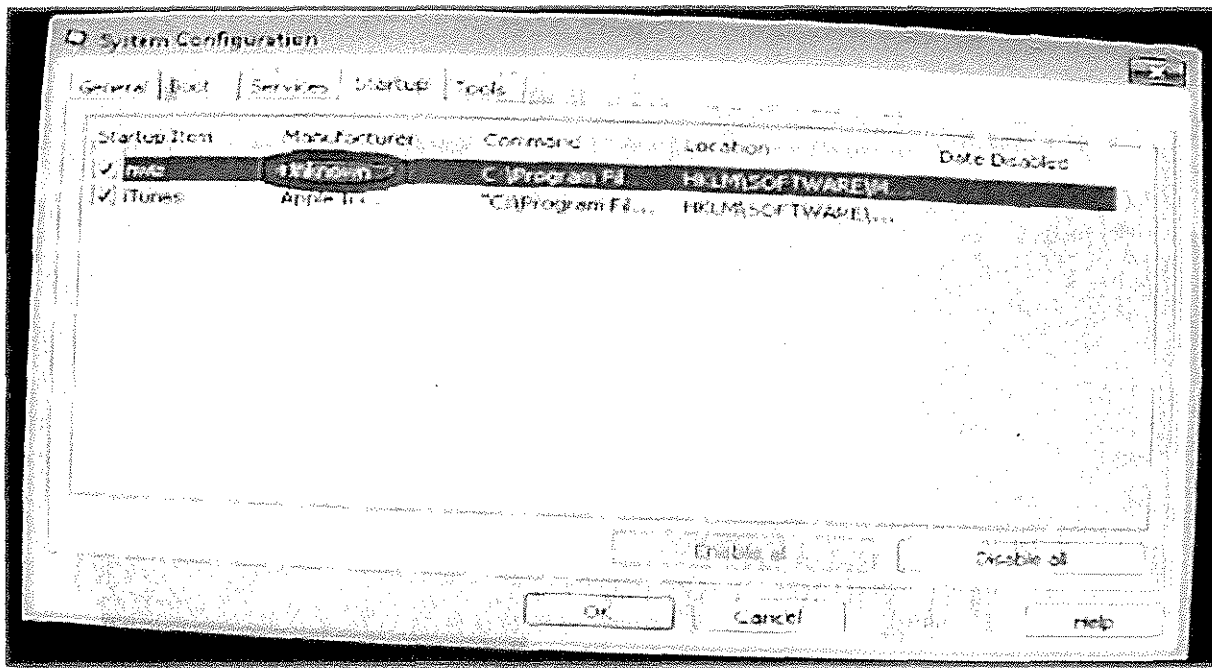
⁴¹ *Id.*

⁴² PX 1, Menjivar Dec. Att. FF at pp. 23-24.

⁴³ *Id.* ¶ 43.

program identified as “nwiz” from an “unknown” manufacturer.⁴⁴ After drawing a red circle around the word “unknown,” as depicted in the screen shot below,⁴⁵ Jake stated:

That’s where the adware is. This isn’t something that you can go and you can uninstall from your programs because this isn’t a program....But this guy right here is the one who’s doing the damage.⁴⁶



Later in the call, Jake claimed that the “adware” he had discovered could only be removed by a “certified technician” at a cost of \$300 from a retailer like Best Buy.⁴⁷ If, however, the investigator agreed to purchase security software from Defendants for \$250, Jake offered to remove the “adware” free of charge.⁴⁸

Jeffrey McJunkin, a computer forensics and security expert retained by Plaintiffs, has analyzed the hard drives and memory captures associated with the computer used in each of

⁴⁴ *Id.* ¶¶ 48-50, 60, Att. GG at p. 20;

⁴⁵ PX 17, McJunkin Dec. ¶ 25.

⁴⁶ PX 1, Menjivar Dec. Att. GG at p. 20. At another point in the call, when asked by the investigator about his level of certainty regarding the purported adware infection, Jake replied: “100 percent you have adware on your computer.” *Id.* at p. 31.

⁴⁷ *Id.* at pp. 29, 32.

⁴⁸ *Id.* at p. 34.

FTC's undercover calls. Mr. McJunkin has concluded that the state of the FTC's computer prior to each undercover call was "uninfected and without security compromise."⁴⁹ Moreover, Mr. McJunkin found that the telemarketers in both calls made misleading statements in their "diagnoses" of the FTC's computer.⁵⁰ In particular, the "SysBank" information identified as evidence of a "virus" that had covertly accessed "banking information" does not, in fact, indicate the presence of a virus or other security problem and has nothing whatsoever to do with a financial bank account.⁵¹ "SysBank" shows the amount of memory installed on the computer.⁵² Similarly, the "unknown" program identified as "adware" by the second telemarketer that could supposedly only be removed by a "certified" technician at a cost of several hundred dollars was actually a legitimate and completely innocuous program associated with the computer's video card.⁵³ In other words, Defendants charged \$500 to the FTC to repair non-existent problems.⁵⁴

The misrepresentations documented above are consistent with transcripts of recorded sales calls obtained by Plaintiffs⁵⁵ as well as sworn testimony provided by consumers⁵⁶ and

⁴⁹ PX 17, McJunkin Dec. ¶ 9.

⁵⁰ *Id.* ¶¶ 13-26.

⁵¹ *Id.*

⁵² *Id.* ¶ 19.

⁵³ Both the program and the card are made by the Nvidia Corporation, a publicly traded technology company based in California. *See Id.* ¶ 26, and <<https://en.wikipedia.org/wiki/Nvidia>>.

⁵⁴ In fact, the "repairs" performed by Defendants rendered the FTC's computer markedly *less* secure. *Id.* ¶¶ 9, 34-35.

⁵⁵ Referring to a program called "Chromium" installed on a consumer's computer, a telemarketer stated: "That's out of Asia...It is fictitious and it's infectious." PX 1, Menjivar Dec. Att. U at p. 7. In reality, Chromium is from Google, not Asia. It is an open-sourced web browser based on the source code for Google's Chrome browser. *Id.* ¶ 23, Att. M. The telemarketer later claimed that he had discovered hackers in the computer as they spoke and pretended to be in the process of expelling them: "I'm still fighting these guys. Give me a second. I'm going to stick in some coding to try to block them off. We have multi-million dollar software we use." *Id.* Att. U at p. 9. *See also id.* Att. X at p. 5 (telemarketer tells consumer that any program identified as "unknown" is "a form of an infection, whether it might be adware or malware"); *id.* Att. Z at p. 7 (telemarketer claims to have discovered something "very, very dangerous" that is storing consumer's "private information" on "cookies").

⁵⁶ PX 5, Best Dec. ¶ 8 (after opening Windows Task Manger and reviewing the number of processes displayed, telemarketer declared that consumer's computer was "under tremendous attack"); PX 6, Brown Dec. ¶ 10 (telemarketer claimed that hackers had accessed consumer's computer through his

Defendants' own employees.⁵⁷ Collectively, this evidence shows that the true purpose of a Help Desk National "diagnostic" is to tell consumers that there is a problem, not to discover whether any problems actually exist. As one employee put it: "Sales reps all understood that this was the only result acceptable to [Help Desk National] management."⁵⁸

3. Defendants Falsely Claim to be Part of, or Certified by, Microsoft and Apple

To earn consumers' trust and create the appearance of legitimacy, Defendants pretend to be part of well-known U.S. technology companies, such as Microsoft or Apple. Defendants also claim to be certified by Microsoft and Apple to service computers running the Windows and OS X operating systems. When, for example, one consumer asked if Help Desk National "made the operating system," the telemarketer responded: "Right, we're with the operating system."⁵⁹ Similarly, during an FTC undercover call, the telemarketer claimed that Help Desk National could offer lower prices than Best Buy "since we're a part of Microsoft."⁶⁰ If a consumer questions Defendants' credibility, the Help Desk National sales script instructs telemarketers to state that they are "partnered with Microsoft" and "certified to service all Microsoft products [and] programs."⁶¹ Telemarketers often claim that only highly trained, "level 3" Microsoft-certified technicians are capable of making the necessary repairs and that Help Desk National

McAfee antivirus software); PX 8, Leahy Dec. ¶ 6 ("unknown" program identified by telemarketer as cause of alleged problem).

⁵⁷ According to former employee Colin Page, the "diagnostic" tests "were simply a means to scare consumers into believing that their computers were in urgent need of repair" and Defendants "required sales reps to fabricate a reason why there was a sign of some alarming problem." PX 16, Page Dec. ¶¶ 19-20. *See also* PX 19, Calaciura Dec. ¶ 17 (former supervisor: "Regardless of the result from the [Webroot] analysis, the consumer was always told there was a serious issue with their computer"); PX 20, Denton Dec. ¶ 22 (former customer service representative: "Consumers were always told that they had a malware infection and that their computer had to be immediately repaired").

⁵⁸ PX 18, Page Dec. ¶ 20.

⁵⁹ PX 11, Zeltser Dec. ¶ 39.

⁶⁰ PX 1, Menjivar Dec. Att. FF at p. 30; *see also id.* Att. GG at p. 47 (referring to "technicians" who would "repair" the FTC's computer, telemarketer claimed: "These guys are Microsoft certified").

⁶¹ *Id.* Att. T at p. 26; PX 18, Page Dec. Att. A at p. 12; PX 19, Calaciura Dec. Att. A at p. 14.

employs individuals with these credentials.⁶² These claims and others like them are an integral part of Defendants' sales pitch and are made repeatedly to consumers.⁶³

In reality, Defendants are not part of Microsoft or Apple, nor are they authorized or certified to provide technical support services for these companies or their products.⁶⁴ Current and former employees have confirmed that the telemarketers who "diagnose" and "repair" problems on consumers' computers have no specialized training or certifications with Microsoft or Apple.⁶⁵ Indeed, as explained in a declaration from a Microsoft representative, the company has not recognized Help Desk National as having any particular or general competency of any sort.⁶⁶

⁶² If, for example, consumers state that they intend to seek help from a friend or family member, Defendants' script directs telemarketers to respond: "You would actually need a Level 3/4/5 Microsoft certified technician to fix this for you." Former employees confirm that telemarketers regularly made these claims. See PX 18, Page Dec. ¶ 23 (telemarketers assured consumers that all repairs were completed by "highly trained" technicians with "level 3" certifications from Microsoft); PX 20, Denton Dec. ¶ 24 (telemarketers "routinely told consumers that the technicians were level three certified with Microsoft, which was not true."). Recorded sales calls obtained by Plaintiffs provide further confirmation. See, e.g., PX 1. Menjivar Dec. Att. U at p. 8 ("I can transfer the session upstairs where the next available level three Microsoft-certified technician does the repair for you..."); *id.* Att. AA at p. 6 ("The only way you can ever repair this computer is to have a level three technician that's Microsoft-certified that knows how to recode your operating system by hand").

⁶³ See, e.g., *id.*, Att. V at p. 4 ("We're Apple-certified technicians, all right"); *id.* Att. X at p. 7 ("We are on [the Microsoft] website because we do all the repair work remotely for their Pinpoint network... We are the biggest tech support company in the world"); *id.* Att. Y at p. 5 ("We're the biggest Microsoft solution provider in the United States"); *id.* at p. 6 (telemarketer transfers consumer to another employee introduced as "literally the top Microsoft-certified security analyst in the country"); *id.* Att. U at p. 5 ("...we are the number one recommended [Microsoft] solution provider in the United States of America"); *id.* Att. W at p. 4 ("infection" on computer is "telling" consumer "to contact Microsoft-certified technicians at the Help Desk"); PX 4, Amos Dec. ¶¶ 5, 11 (telemarketer told consumer that he was a Microsoft technician and that Defendants "worked with Microsoft"); PX 5, Best Dec. ¶ 7 (consumer told that Help Desk National "was comprised of Microsoft-recommended technicians"); PX 6, Brown Dec. ¶ 9 (telemarketer claimed that Help Desk National was "Microsoft-certified").

⁶⁴ See PX 14, Declaration of Julie Crawford, Corporate Procurement Manager, Apple Inc. ¶ 5 (Defendants not authorized or certified to service Apple products); PX 15, Aebi Dec. ¶ 9 (Defendants not authorized or certified to service Microsoft products).

⁶⁵ See PX 18, Page Dec. ¶ 23; PX 20, Denton Dec. ¶ 24.

⁶⁶ See PX 15, Aebi Dec. ¶ 8. Through their d/b/a Help Desk National, Defendants are registered with the Microsoft Partner Network as a "Network Member," the most basic membership tier available. *Id.* ¶ 4. This means that Help Desk National appears in Pinpoint, a searchable online directory maintained by Microsoft of third parties that provide services related to Microsoft products. It does *not* mean that

4. Closing the Sale

After completing their “diagnostic,” Defendants present consumers with two “repair” options. First, to create the appearance that they are unbiased experts only concerned with helping consumers, Defendants suggest that consumers can take their computers for repair to a nearby Best Buy, Office Depot, or Staples.⁶⁷ In accordance with their script, Defendants even instruct many consumers to provide the store technician with a list of three tasks that “need” to be completed.⁶⁸ Defendants warn consumers that store repair will take there- to five-“business days” and cost at least three hundred dollars.⁶⁹ At this point, Defendants introduce the second option – they offer to perform the needed repairs remotely at a lower price while consumers relax in the comfort of their own homes.⁷⁰ Defendants then charge \$200-\$300 to “repair” consumers’ computers.⁷¹

In addition to repair services, Defendants also pressure consumers into spending hundreds of dollars for security software. Defendants train their telemarketers to claim that any

Defendants have attained specialized training or certification from Microsoft, or that they have a distinctive relationship with Microsoft. To the contrary, there are over 200,000 Network Members. *Id.* Moreover, Network Members do not need to pass any certifications and there is no cost for a company to join at this level. *Id.*

⁶⁷ See PX 18, Page Dec. ¶ 21; PX 19, Calaciura Dec. ¶ 18; PX 20, Denton Dec. ¶ 23.

⁶⁸ PX 1, Menjivar Dec. Att. T at p. 5; PX 19, Calaciura Dec. Att. A at p. 5. These tasks, which Defendants claim must be completed “manually using a Certified Technician,” include: 1) “remove unwanted programs”; 2) “cleanup running services”; and 3) “a full system tune-up.” *Id.*

⁶⁹ *Id.* See also PX 5, Best Dec. ¶ 10 (in-store repair time estimated at one week to ten days); PX 7, Law Dec. ¶ 13 (consumer told that Best Buy repair would take longer and be more expensive); PX 10, Salafrio Dec. ¶ 10 (telemarketer offered to “fix” consumer’s computer for \$50 less than what she would be charged by Office Depot).

⁷⁰ See, e.g., PX 1, Att. T at p. 5 (script); PX 5, Best Dec. ¶¶ 10-11 (consumer); PX 18, Page Dec. ¶ 22 (former employee).

⁷¹ See PX 1, Menjivar Dec. ¶¶ 43, 51; PX 4, Amos Dec. ¶ 6 (\$300); PX 5, Best Dec. ¶ 11 (\$250); PX 6, Brown Dec. ¶ 11 (\$300); PX 8, Leahy Dec. ¶ 5 (\$202); PX 9, Lerch Dec. ¶ 7 (\$200); PX 10, Salafrio Dec. ¶ 8 (\$250); PX 11, Zeltser Dec. ¶ 47 (\$250); PX 18, Page Dec. ¶ 24 (according to former employee, prices ranged from \$200 to \$300). Defendants often claim that the “infections” they discover on consumers’ computers can spread to other devices sharing the same network. They then offer, for an additional fee, to “repair” other computers owned by the same consumers. See, e.g., PX 1, Menjivar Dec. Att. Z at p. 11 (“You’re familiar, of course, with the fact that this stuff can cross-contaminate as well”); PX 4, Amos Dec. ¶ 11 (representative claimed that malware can “jump” from one computer to another).

antivirus program currently running on consumers' computers is worthless because it is "reactive."⁷² According to Defendants, "reactive" software from well-known developers like Norton, AVG, Kaspersky, and McAfee will allow infections onto a computer and then attempt to remove them after the fact.⁷³ By contrast, Defendants assert, their software is "proactive" and will stop threats before they manage to find their way onto consumers' computers.⁷⁴ This distinction, according to Plaintiffs' expert, is groundless.⁷⁵ Moreover, the software pushed by

⁷² The following statement from Defendants' script is tailored to accommodate whatever antivirus software happens to be installed on a consumer's computer and then advocate replacing it with whatever alternative Defendants happen to be selling at the time: "Most security professionals are aware of the two basic approaches used to deal with security vulnerabilities: proactive and reactive. You're using _____ ANTI VIRUS. That's [sic] a good program but it is reactive. It allows threat on your computer then runs a scan to remove them. I use a program called _____ that's [sic] an active security that will stop a threat before it gets on your machine." PX 1, Menjivar Dec. Att. T at p. 3. Defendants sell, or have sold, a variety of different antivirus and security programs, including a white-labeled product they market as "Magnum Anti-Malware." See also PX 1, Menjivar Dec. ¶¶ 42, 50; PX 19, Calaciura Dec. ¶ 19; PX 20, Denton Dec. ¶ 23.

⁷³ Defendants require telemarketers to tell consumers that their current antivirus software is "garbage." PX 18, Page Dec. ¶ 25. See, e.g., PX 1, Menjivar Dec. Att. W at pp. 10-11 (Kaspersky antivirus software is the equivalent of having "no protection at all"); *id.* Att. X at p. 4 (telemarketer claims that AVG, McAfee and Norton "used to be good about 10 to 15 years ago" but are no longer able to protect against "the more severe attacks that we are dealing with now"); PX 6, Brown Dec. ¶ 10 (telemarketer claimed McAfee was not capable of protecting consumer's computer because it is "defensive"); PX 9, Lerch Dec. ¶ 6 (telemarketer characterized McAfee as "inadequate, outdated, and not capable of stopping new threats").

⁷⁴ See, e.g., PX 1, Menjivar Att. U at p. 10 (telemarketer claims that Watchdog Anti-Malware is "the number one ranked proactive security software on the globe"); *id.* Att. FF at p. 35 (telemarketer claims that he has consulted with Defendants' "security software team," which has determined that FTC investigator must purchase "Magnum Security"); *id.* Att. GG at p. 34 (telemarketer urges FTC investigator to purchase "Magnum Anti-Malware" because "it's proactive software that will stop the infections before they get in").

Some telemarketers take this ruse a step further, leading consumers to believe that Defendants' antivirus products are endorsed or made by Microsoft. See, e.g., PX 11, Zeltser Dec. ¶¶ 22-23 (telemarketer claims that "STOPZilla" is superior to Norton and McAfee because it is a "Microsoft Silver product" developed by Microsoft itself); PX 1, Menjivar Dec. Att. Z at 10 (telemarketer recommends purchase of two programs that are "the only stuff that works" and that are "backed by the Microsoft Pinpoint Network").

⁷⁵ PX 17, McJunkin Dec. ¶ 34.

Defendants is available for a fraction of the cost from legitimate retailers or, in the case of their Apple product, a free download.⁷⁶

Consumers who balk at purchasing Defendants' repair services or security software are deceived, scared, shamed, and even berated into doing so. Defendants typically invoke the menace of hackers stealing consumers' sensitive personal and financial information, which Defendants claim is a virtual certainty if consumers refuse to heed Defendants' advice.⁷⁷ These practices are especially troubling in light of Defendants' systematic targeting of elderly consumers,⁷⁸ as illustrated by the following exchange:

TELEMARKETER: Please don't disrespect me by telling that you don't have \$300. This is the United States of America, okay? You've living in a place that's \$3,000 a week to live in. You have \$300. Please don't disrespect me like that.

CONSUMER: I live in a nursing home. I live in a nursing home and Medicare pays for it....

TELEMARKETER: Good. Then that's excellent because then you have money then if they're paying for it.⁷⁹

⁷⁶ There is one Avast product available in the U.S. for Apple computers and it is free. PX 16, Declaration of Kelby Barton, Deputy General Counsel, Avast Software s.r.o ¶ 3. Defendants charge hundreds of dollars to consumers for a comparable product and do so without authorization from Avast. *See id.* ¶¶ 3-4; PX 1, Menjivar Dec. Att. J at 11 (\$299), Att. K at p. 10 (\$499), Att. P at p. 8 (\$300), Att. V at p. 6 (\$449). Similarly, Defendants charge as much as \$499 for a product known as Watchdog Anti-Malware, and \$150 for Defender Pro, *see id.* Att. K at p. 9 and Att. P at p. 8, which are available from Amazon for \$39.99 and \$14.99 respectively. *Id.* ¶¶ 24-25.

⁷⁷ PX 1, Menjivar Dec. Att. W at p. 10 (speaking to 90-year old consumer with Kapersky anti-virus program installed on his computer, telemarketer states: "I can tell you this, now, Bob. You have no protection at all on this computer. This is going to keep happening if you do not buy the proper protection."); *id.* Att. Y at p. 3 (telemarketer to consumer living in nursing home unsure whether he can afford Defendants' \$300 "repair" fee: "You have a malware infection that's on here that is trying to steal your personal information"); *id.* Att. Z at p. 10 (telemarketer claims to have identified "very, very dangerous" threat indicating that hackers are "attempting to steal your credit card" and "Social security number"); *id.* Att. AA at p. 4 (telemarketer warns that consumer's computer is infected with "very malicious browser hijacker" that will steal her personal information and "completely corrupt your operating system"); PX 18, Page Dec. ¶ 28 (telemarketers regularly used "flagrantly deceptive claims" and "extremely high-pressure sales tactics" to meet Defendants' sales quotas); PX 20, Denton Dec. ¶ 20 (telemarketers used high-pressure sales tactics to scare consumers into paying for repairs and software).

⁷⁸ *See* PX 18, Page Dec. ¶¶ 10, 17, 28 (former employee).

⁷⁹ PX 1, Menjivar Dec. Att. Y at p. 3. The telemarketer later demanded that the consumer contact his bank to lift a fraud hold so that Defendants could charge his credit card. *Id.* at p. 4.

Defendants' treatment of this consumer is not an isolated incident.⁸⁰

C. Consumer Injury

Defendants' illegal conduct has caused millions of dollars in consumer harm. This harm, along with the scale of Defendants' operation, is reflected in records obtained from the service that enables telemarketers to gain remote access to consumers' computers. These records show that between January 2015 and May 2016, Defendants initiated 342,787 remote access sessions.⁸¹ During this same time frame, Defendants paid over \$5.5 million to run their call center as well as an additional \$2 million to generate leads with their deceptive pop-ups and chatbots.⁸²

III. DEFENDANTS

Defendants are six corporations and the six individuals who own, direct, and manage this scheme as well as share in its profits. They are located in three U.S. states (Florida, Nevada, and Iowa) as well as in Canada. As described below, five of these corporations operate as a common enterprise.

A. Florida Defendants

The Florida-based Defendants operate Help Desk National's call center in Boynton Beach. Consumers who dial numbers found on Defendants' pop-up and chatbots reach a telemarketer at this location.⁸³ Defendant **Christopher J. Costanza** has been identified by former employees as one of the owners of Help Desk National as well as the manager of its call

⁸⁰ See, e.g., *id.* Att. W at p. 6 (telemarketer speaking to a 90-year old consumer: "...you're being stubborn and you're not doing something you know that you could do, okay? So...let's be an adult here. This is easy, easy stuff").

⁸¹ *Id.* ¶ 19.

⁸² *Id.* ¶¶ 13, 61.

⁸³ Defendants also maintain a second location in Boynton Beach for training new employees. PX 19, Calaciura Dec. ¶ 3.

center.⁸⁴ Costanza has procured telecommunications services and Internet domain names used by Defendants.⁸⁵ He is also a signatory on corporate bank accounts used to facilitate the operation.⁸⁶ Finally, Costanza is the principal of corporate defendants Big Dog Solutions LLC, PC Help Desk US LLC, and Inbound Call Specialist LLC.⁸⁷

Suzanne W. Harris is an officer of corporate defendants Big Dog Solutions and PC Help Desk US LLC.⁸⁸ Harris is also a signer on several bank accounts maintained by Big Dog Solutions.⁸⁹ A former employee has identified her as the bookkeeper for Defendants' call center.⁹⁰

Defendants operate their call center through corporate defendants Big Dog Solutions LLC, PC Help Desk US LLC, and Inbound Call Specialist LLC, all of which are Florida limited liability companies.⁹¹ **Big Dog Solutions** has received \$5.5 million in proceeds of Defendants' scam and pays all expenses associated with the operation of its call center, including payroll, rent, telecommunication services, Internet services, and remote access services.⁹² **PC Help Desk US LLC** is located at the same address as Big Dog Solutions and does business as Help Desk National.⁹³ It has maintained a website (www.pchelpdeskus.com) advertising technical support services that displays a telephone number registered to Big Dog Solutions.⁹⁴ **Inbound Call**

⁸⁴ See PX 18, Page Dec. ¶¶ 6, 15; PX 19, Calaciura Dec. ¶ 3; PX 20, Denton Dec. ¶¶ 3, 5, 11.

⁸⁵ See PX 1, Menjivar Dec. ¶¶ 14, 17. Costanza is the registrant of domain names used by corporate defendants Big Dog Solutions LLC (www.bigdogsolutions.org) and PC Help Desk US LLC (www.pchelpdeskus.com). *Id.* ¶¶ 14(a), 20, Att. J.

⁸⁶ *Id.* ¶¶ 9-10, Att. G.

⁸⁷ *Id.* ¶ 5, Atts. A-C.

⁸⁸ *Id.* ¶ 5, Att. A, B.

⁸⁹ *Id.* ¶ 9, Att. G.

⁹⁰ PX 18, Page Dec. ¶ 6.

⁹¹ PX 1, Menjivar ¶ 5, Atts. A-C.

⁹² *Id.* ¶¶ 9-10, 61.

⁹³ *Id.* ¶ 5, Att. B; *id.* Att. J at p. 23 (terms of service for PC Help Desk website identify company as "Help Desk National"); *id.* ¶ 20 (PC Help Desk website links to Help Desk National's Microsoft Pinpoint profile).

⁹⁴ *Id.* ¶ 17(c) and Att. J (website displays contact number registered to Big Dog Solutions).

Specialist LLC provides consulting and marketing services to Defendants.⁹⁵ Costanza and Harris have made over \$125,000 in cash withdrawals from a bank account maintained by Inbound Call Specialist.⁹⁶

B. Canadian Defendants

Three individuals named in Plaintiffs' complaint are residents of Canada: Gary Oberman, Muzaffar Abbas, and Donald Dolphin.⁹⁷ They control corporate defendant **9138242 Canada Corporation**, which is based in Montreal, Quebec.⁹⁸ Proceeds of Defendants' scam are transferred to 9138242 Canada, which then disburses these funds to defendants Big Dog Solutions and BlackOptek CE to cover the costs of operating Defendants' call center and disseminating their misleading advertisements.⁹⁹

Gary Oberman, along with Costanza, oversees daily operations of Help Desk National.¹⁰⁰ He is a director of 9138242 Canada and the registrant of several websites used in connection with Defendants' scheme.¹⁰¹ Oberman is a contact for Defendants'

⁹⁵ *Id.* ¶ 11(b).

⁹⁶ *Id.*

⁹⁷ *Id.* ¶ 6, Att. D.

⁹⁸ *Id.*

⁹⁹ Although Plaintiffs do not have records from Defendants' merchant processors or the bank account that received payouts from these processors, it is possible to trace the flow of funds obtained from consumers through records subpoenaed from banks used to facilitate this scheme. Based on these records, it appears that proceeds from Defendants' merchant accounts were deposited into a bank account maintained in Canada by corporate defendant 9138242 Canada Inc. From here, these funds were disbursed to accounts in the U.S. maintained by corporate defendants BlackOptek CE Inc., Big Dog Solutions LLC, and Digital Growth Properties LLC. *See id.* ¶ 61 (between January 28, 2015 and May 31, 2016, Big Dog Solutions received 99 wire transfers totaling \$5,558,300 from 9138242 Canada); *id.* ¶ 13(a) (34 wire transfers totaling \$2,697,320 received by BlackOptek CE from 9138242 Canada during comparable time frame); *id.* 13(b) (35 wire transfers totaling \$2,124,063 received by Digital Growth Properties from BlackOptek CE during comparable time frame).

¹⁰⁰ *See* PX 11, Zeltser Dec. ¶¶ 52-54, Att. H (conversation between Oberman and computer security expert and blogger, Lenny Zeltser, in which Oberman speaks on behalf of Help Desk National and confirms that he controls Defendants' marketing); PX 19, Calacirua Dec. ¶ 19 (Oberman identified as owner by former supervisor, who also states that Oberman obtained antivirus software marketed by Defendants to consumers).

¹⁰¹ *See* PX 1, Menjivar Dec. ¶ 6, Att. D; *id.* ¶ 14(b).

telecommunications service provider and he registered Help Desk National with the Microsoft Pinpoint network.¹⁰²

Muzaffar Abbas is a director of 9138242 Canada and the chief executive officer of corporate defendant BlackOptek CE Inc.¹⁰³ Abbas manages advertising and lead generation for Help Desk National, including the pop-ups and chatbots that lure consumers into contacting Defendants' call center.¹⁰⁴ He is the primary contact for a company hired by Defendants to provide call tracking and analytics for their marketing campaigns.¹⁰⁵ He also controls the corporate bank account that funds Defendants' marketing operations.¹⁰⁶

Donald Dolphin is a director of 9138242 Canada and the chief operating officer of BlackOptek CE Inc.¹⁰⁷ He has registered several websites used by Defendants, including www.helpdesknational.com.¹⁰⁸

C. Nevada Defendant

BlackOptek CE Inc. is a Nevada corporation controlled by individual defendants Abbas and Dolphin.¹⁰⁹ It has received millions of dollars from defendant 9138242 Canada and disbursed these funds to defendant Digital Growth Properties and other third parties responsible for lead generation.¹¹⁰ BlackOptek also procures telecommunication services for Defendants, including the numbers that appear in their pop-up and chatbot advertisements.¹¹¹

¹⁰² *Id.* ¶¶ 62, Att. HH.

¹⁰³ *Id.* ¶¶ 6-7, Atts. D, E.

¹⁰⁴ PX 19, Calaciura Dec. ¶¶ 7-8.

¹⁰⁵ PX 1, Menjivar Dec. ¶¶ 15-16.

¹⁰⁶ *Id.* ¶¶ 12-13, Att. H.

¹⁰⁷ *Id.* ¶¶ 6-7, Atts. D, E.

¹⁰⁸ *Id.* ¶¶ 14(c), 21, Att. K.

¹⁰⁹ *Id.* ¶ 7, Att. E.

¹¹⁰ *Id.* ¶¶ 12-13.

¹¹¹ *Id.* ¶¶ 16-17, Att. I.

D. Iowa Defendants

Justin Powers and his company, **Digital Growth Properties, LLC**, are responsible for disseminating the vast majority of misleading pop-up and chatbot ads used by Defendants for lead generation. These advertisements appear on websites registered to Powers and Digital Growth, and those two have received in excess of \$2 million from Defendants for these services.¹¹² In addition to managing lead generation for Defendants, Powers also plays a role in Help Desk National's telemarketing operations. He has visited Defendants' Florida call center at least once with Abbas and was identified by a former employee as an owner of the business.¹¹³

E. Common Enterprise

Five of the six named corporate defendants operate as a common enterprise and are therefore jointly and several liable for each other's illegal conduct. To determine if a common enterprise exists, courts consider various factors, including: (1) maintaining officers and employees in common; (2) operating under common control; (3) sharing of office space; (4) operating the business through a maze of interrelated companies; (5) comingling of funds; and (6) sharing of advertising and marketing. *FTC v. Wash. Data Res.*, 856 F. Supp. 2d 1247, 1271 (M.D. Fla. 2012) (citations omitted). Corporate Defendants Big Dog Solutions, PC Help Desk US, Inbound Call Experts, 9138242 Canada, and BlackOptek CE meet this test.

Big Dog Solutions, PC Help Desk US, and Inbound Call Specialist share office space, common officers, and business functions.¹¹⁴ 9138242 Canada funds the operations of BlackOptek and Big Dog Solutions from merchant account payments.¹¹⁵ All five companies

¹¹² *Id.* ¶¶ 14(d), 27-28, Atts. Q-S (Defendants' chatbot advertisements are connected to URLs registered to Powers); *id.* ¶ 13(b).

¹¹³ PX 19, Calaciura Dec. ¶¶ 7-8

¹¹⁴ All three entities operate out of 2240 W. Woolbright Road, Suite 205 in Boynton, Beach, Florida. *See* PX 1, Menjivar Dec. ¶¶ 5, 11(h), Atts. A and B.

¹¹⁵ *See* note 99, *supra*.

commingle assets, operate through the same series of pop-up ads, websites, and telephone numbers, and jointly operate a single tech support scam.¹¹⁶

IV. ARGUMENT

Defendants' practices violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), the Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310, and Section 501.204 of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Chapter 501, Part II, Florida Statutes. To prevent any further injury to consumers, the FTC and State of Florida ask that the Court issue *ex parte* their proposed TRO. This order would enjoin Defendants' ongoing law violations and would provide for other equitable relief designed to preserve the Court's ability to provide restitution to victims at the conclusion of the case.

A. The Court Has the Authority to Grant the Requested Relief

The FTC Act provides that "in proper cases the Commission may seek, and after proper proof, the court may issue, a permanent injunction." 15 U.S.C. § 53(b). Once the Commission invokes the federal court's equitable powers, the full breadth of the court's authority is available, including the power to grant such ancillary final relief as rescission of contracts and restitution. *FTC v. Febre*, 128 F.3d 530, 534 (7th Cir. 1997); *FTC v. Amy Travel Serv., Inc.*, 875 F.2d 564, 571-72 (7th Cir. 1989). The court may also enter a temporary restraining order, a preliminary injunction, and whatever additional preliminary relief is necessary to preserve the possibility of providing effective final relief. *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1026 (7th Cir. 1988); *see also Amy Travel*, 875 F.2d at 571. Such ancillary relief may include a

¹¹⁶ For example, BlackOptek pays a third party, Invoca, for call tracking and data analytics services used by Defendants to manage their advertising campaigns. *See* PX 1, Menjivar Dec. ¶¶ 13(c), 15-16. This service enables the phones in the Help Desk National call center -- run by Big Dog Solutions and funded by 9138242 Canada -- to display the name of the campaign that generates an incoming call. *See* PX 18, Page Dec. ¶ 13 (as explained by a former telemarketer, "if my caller ID displayed the message 'Jake Anderson,' I knew that the person calling had encountered the Jake Anderson chatbot" and would tailor his opening pitch accordingly).

temporary restraining order that freezes assets for consumer restitution, appoints a temporary receiver, and allows immediate access to business premises. *World Travel*, 861 F.2d at 1031. Courts in the Seventh Circuit have regularly issued the type of preliminary relief sought here against businesses, like that of Defendants, that are permeated by fraud.¹¹⁷

This Court has personal jurisdiction over all of the Defendants, and venue is proper here. Because Defendants have minimum contacts with the United States, the Court has personal jurisdiction over them under the FTC Act's nationwide service of process provision, 15 U.S.C. § 53(b). See *FTC v. Cleverlink Trading Ltd.*, No. 05-cv-2889, 2006 WL 1735276, at *4 (N.D. Ill. June 19, 2006) (Kendall, J.); *FTC v. Bay Area Bus. Council, Inc.*, No. 02-cv- 5762, 2003 WL 21003711, at *2 (N.D. Ill. May 1, 2003) (Darrah, J.). Moreover, under the FTC Act's venue provision, an action may be brought wherever a corporation "resides or transacts business." 15 U.S.C. § 53(b). Here, as shown by their customer service call records, Defendants have transacted substantial business in this district.¹¹⁸ In addition, venue is proper over a corporation wherever it is subject to personal jurisdiction. See *Bay Area*, 2003 WL 21003711, at *2.

B. Plaintiffs Meet the Standard for Issuance of a Temporary Restraining Order

To grant preliminary injunctive relief in an FTC Act case, the district court must:

- (1) determine the likelihood that the Commission will ultimately succeed on the merits, and
- (2) balance the equities. *World Travel*, 861 F.2d at 1029. Under this "public interest" test, "it is not necessary for the FTC to demonstrate irreparable injury." *Id.* When the court balances the equities, the public interest "must receive far greater weight" than any private concerns. *Id.*

¹¹⁷ See note 122, *infra*.

¹¹⁸ PX 1, Menjivar Dec. ¶ 18 (call detail records showing 1,464 calls from area codes within the Northern District of Illinois to Defendants' customer service telephone numbers). See also PX 6, Brown Dec. (declaration from consumer victim who resides in Chicago).

1. Plaintiffs are Likely to Succeed on the Merits

a. Deceptive Sales Practices in Violation of the FTC Act (Counts I and II)

Defendants' widespread misrepresentations violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) and the FDUTPA, which each prohibit deceptive acts or practices in or affecting commerce. An act or practice is deceptive if it involves a material misrepresentation or omission that is likely to mislead consumers acting reasonably under the circumstances. *See FTC v. Bay Area Bus. Council, Inc.*, 423 F.3d 627, 635 (7th Cir. 2005); *FTC v. World Media Brokers*, 415 F.3d 758, 763 (7th Cir. 2005); *FTC v. QT, Inc.*, 448 F. Supp. 2d 908, 957 (N.D. Ill. 2006). The materiality requirement is satisfied if the misrepresentation or omission involves information that is likely to affect a consumer's choice of, or conduct regarding, a product or service. *See Kraft, Inc. v. FTC*, 970 F.2d 311, 322 (7th Cir. 1992). Express claims, or deliberately made implied claims, used to induce the purchase of a particular product or service are presumed to be material. *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1096 (9th Cir. 1994); *FTC v. SlimAmerica, Inc.*, 77 F. Supp. 2d 1263, 1272 (S.D. Fla. 1999). In deciding whether particular statements are deceptive, courts must look to the "overall net impression" that the statements create. *See Kraft*, 970 F.2d at 322; *FTC v. Stefanchik*, 559 F.3d 924, 928 (9th Cir. 2009).

The FTC need not prove that a defendant made misrepresentations with an intent to defraud or deceive, or in bad faith. *FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1202 (10th Cir. 2005). Nor does the FTC need to show actual reliance by consumers; it is enough that the representations were likely to be relied on by consumers acting reasonably under the circumstances. *See FTC v. Verity Int'l, Ltd.*, 443 F.3d 48, 63 (2d Cir. 2006); *FTC v. Figgie Int'l, Inc.*, 994 F.2d 595, 605 (9th Cir. 1993) ("Requiring proof of subjective reliance by each individual consumer would thwart effective prosecutions of large consumer redress actions and

frustrate the goals of [Section 13(b)].”); *FTC v. Sec. Rare Coin & Bullion Corp.*, 931 F.2d 1312, 1316 (8th Cir. 1991). “[A] presumption of actual reliance arises once the FTC has proved that the [d]efendant made material misrepresentations, that they were widely disseminated, and that consumers purchased the [d]efendant’s product.” *Figgie Int’l*, 994 F.2d at 605-06.

As shown above in great detail, Defendants make two broad types of representations to induce consumers to purchase technical support services and software: first, Defendants claim that they are part of well-known technology companies, such as Microsoft or Apple, or are certified or authorized to service products made by these companies; second, Defendants claim that they have detected security or performance issues on consumers’ computers, including viruses, malware, or the presence of hackers.

Both of these core representations are false and unquestionably material. Defendants make these misrepresentations for the specific purpose of causing consumers to believe that there is something wrong with their computers and that Defendants can be trusted to fix these problems. These misrepresentations lead consumers to call Defendants and allow their computers to be accessed, which, in turn, enables Defendants to run their phony “diagnostic” and scare consumers into paying hundreds of dollars for Defendants’ products and services. Absent these false claims, a reasonable consumer would not do business with Defendants, who are not authorized to service Microsoft and Apple products, and who have no idea whether there actually is anything wrong with consumers’ computers.

Defendants’ misrepresentations are likely to mislead reasonable consumers that Help Desk National is part of Microsoft or Apple, or authorized by these companies to service their products. As detailed by the declarations and other evidence submitted by Plaintiffs, consumers form this belief because Defendants, in their sales pitch, repeatedly invoke the names of these

companies. They also falsely reassure consumers that Help Desk National and its “technicians” have received specialized training and certifications from Microsoft and Apple. Finally, Defendants tout their status as a member of the Microsoft Pinpoint network, but fail to disclose that membership at their level (the lowest tier available) is free and, in Defendants’ case, does not signify that they are certified, trained, or endorsed by Microsoft.

Consumers also reasonably believe that their computers are in need of immediate repair. Defendants go to great lengths to ensure this. They disseminate advertisements designed to look like security warnings from consumers’ computers or non-existent technical support representatives (which, in many cases, actually prevent those computers from functioning properly); they gain remote access to computers and misrepresent the significance of innocuous messages, files, and information found on those computers; and they claim unequivocally that the failure to purchase Defendants’ repair services and security software will not only cause permanent damage to consumers’ computers, but expose their sensitive personal information to hackers. Given the extent and complexity of these ruses, as well as the number of consumers deceived by them, Defendants’ claims are likely to mislead reasonable consumers.

b. Violations of the Telemarketing Sales Rule (Counts III and IV)

The TSR prohibits any seller or telemarketer from making a false or misleading statement to induce any person to pay for goods or services. 16 C.F.R. § 310.3(a)(4). Defendants are sellers or telemarketers as defined by the TSR because they arrange for the sale of goods or services. 16 C.F.R. § 310.2(dd), (ff), & (gg). As explained above, Defendants falsely claim that they: 1) are part of Microsoft or Apple, or certified by these companies to service their products; and 2) have detected security or performance issues on consumers’ computers. Defendants make these statements to induce consumers to purchase technical support services and security

software and have, in fact, generated millions of dollars in revenue from this conduct. Therefore, Defendants have violated the TSR.

c. Violation of the Florida Deceptive and Unfair Trade Practices Act (Counts V and VI)

Section 501.204 of the FDUTPA, Chapter 501, Part II, prohibits unfair or deceptive acts or practices in the conduct of any trade or commerce. The same representations that violate Section 5 of the FTC Act also violate the Florida Deceptive and Unfair Trade Practices Act, which tracks the language of the FTC Act and prohibits deceptive acts or practices. In construing this Section, the Florida Legislature has declared that “due consideration and great weight shall be given to the interpretation of the Federal Trade Commission and the federal courts relating to the Section 5(a)(1) of the Federal Trade Commission Act, § 45(a)(1) as of July 1, 2006.” *Id.*

2. The Balance of Equities Strongly Favors Injunctive Relief

Once the FTC has shown a likelihood of success on the merits, the Court must balance the equities, giving greater weight to the public interest than to any of Defendants’ private concerns. *World Travel*, 861 F.2d at 1029. The public equities here are compelling, as the public has a strong interest in halting the deceptive scheme, and in preserving the assets necessary to provide effective final relief to victims. *See FTC v. Sabal*, 32 F. Supp. 2d 1004, 1009 (N.D. Ill. 1998). Defendants, by contrast, have no legitimate interest in continuing to deceive consumers and persisting with conduct that violates federal law. *See id.*; *FTC v. World Wide Factors, Ltd.*, 882 F.2d 344, 347 (9th Cir. 1989) (upholding district court finding of “no oppressive hardship to defendants in requiring them to comply with the FTC Act, refrain from fraudulent representation or preserve their assets from dissipation or concealment.”). An

injunction is necessary to ensure that Defendants do not continue their scheme while the case is pending.

C. The Individual Defendants are Liable for the Practices of the Corporate Defendants

The individual defendants are responsible for the illegal activity of the corporations they control.¹¹⁹ An individual may be held liable for injunctive and monetary relief under the FTC Act if the individual: (1) participated directly in or had authority to control the practices, and (2) had some knowledge of the practices. See *Bay Area Bus. Council*, 423 F.3d at 636; *World Media Brokers*, 415 F.3d at 764; *Amy Travel Serv., Inc.*, 875 F.2d at 573.¹²⁰ Authority to control may be evidenced by “active involvement in business affairs and the making of corporate policy, including assuming the duties of a corporate officer.” *Amy Travel*, 875 F.2d at 573. The FTC does not need to show intent to defraud. *Id.*

Each individual is an officer of one or more of the corporate defendants, giving rise to a presumption of control. Voluminous evidence submitted by Plaintiffs show the direct involvement of these individuals in managing their call center, hiring and supervising employees, disseminating misleading advertising, and obtaining services used to facilitate the Help Desk

¹¹⁹ As noted above in Section III, *supra*, five of the six corporate defendants do not function as independent legal entities, but as an interrelated network to facilitate Defendants’ scam. They are therefore jointly and severally liable for Defendants’ conduct because they have operated as a common enterprise. See *Del. Watch v. FTC*, 332 F.2d 745, 746 (2nd Cir. 1964); *accord FTC v. J.K. Publ’ns., Inc.*, 99 F. Supp. 2d 1176, 1202 (C.D. Cal. 2000); *FTC v. Wash. Data Res.*, 856 F. Supp. 2d 1247, 1271 (M.D. Fla. 2012); *FTC v. Direct Benefits Group, LLC*, 6:11-cv-1186-Orl-28TBS, 2013 WL 3771322, at *18 (M.D. Fla. July 18, 2013). As also described above, the remaining sixth corporate defendant, Digital Growth Properties, has received millions of dollars for its role in circulating the advertisements disguised as security alerts that lure consumers into contacting Defendants’ call center. These ads incorporate the two core misrepresentations alleged in Plaintiffs’ complaint and are an integral part of Defendants’ telemarketing scheme. Digital Growth Properties should therefore be held liable for all of the conduct attributable to Defendants.

¹²⁰ The knowledge requirement is satisfied by a showing that the defendant (1) had actual knowledge of the deceptive acts or practices, (2) was recklessly indifferent to the truth or falsity of the representations, or (3) had an awareness of a high probability of fraud coupled with an intentional avoidance of the truth. See *World Media Brokers*, 415 F.3d at 764; *Bay Area Bus. Council*, 423 F.3d at 636; *Amy Travel*, 875 F.2d at 574.

National operation. Given their control over and active participation in this scheme, the individual defendants are undoubtedly aware of the deceptive practices, and should therefore be held individually liable.

D. The Scope of the Proposed Temporary Restraining Order is Necessary and Appropriate

An *ex parte* TRO is necessary and legally appropriate to prevent Defendants from dissipating assets and destroying evidence. Plaintiffs respectfully request a TRO to: (a) freeze Defendants' assets; (b) appoint a temporary receiver over the corporate defendants; and (c) grant Plaintiffs immediate access to Defendants' records and information. Defendants are likely to dissipate assets or destroy evidence if given advance notice of the FTC's action.¹²¹ Courts in this district have frozen defendants' assets, appointed receivers, and granted the FTC immediate access to defendants' business premises in numerous FTC enforcement actions.¹²²

1. Asset Freeze

An asset freeze is appropriate once the Court determines that the FTC is likely to prevail on the merits and that restitution would be an appropriate final remedy. *See World Travel*, 861 F.2d at 1031 & n.9. The district court at that juncture has "a duty to ensure that the assets of the

¹²¹ See Declaration and Certification of FTC Counsel Pursuant to Fed. R. Civ. P. 65(b) in Support of Plaintiffs' *Ex Parte* Motion for Temporary Restraining Order and Motion to Temporarily Seal File (describing need for *ex parte* relief and citing cases in which defendants who learned of impending FTC action withdrew funds, destroyed vital documents, and fled the jurisdiction).

¹²² See, e.g., *FTC v. Stark Law, LLC et al.*, No. 16-cv-3463 (N.D. Ill. Mar. 26, 2016) (Pallmeyer, J.) (*ex parte* TRO with asset freeze and appointment of a receiver); *FTC v. Caprice Marketing LLC et al.*, No. 13-cv-6072 (N.D. Ill. Aug. 27, 2013) (Lee, J.) (*ex parte* TRO with asset freeze); *FTC v. Apogee One Enterprises LLC et al.*, No. 12-cv-588 (N.D. Ill. Jan. 26, 2016) (Kennelly, J.) (*ex parte* TRO with asset freeze and appointment of a receiver); *FTC v. Yellow Page Mktg., B.V., et al.*, No. 11-cv-05035 (N.D. Ill. July 26, 2011) (Leinenweber, J.) (*ex parte* TRO with asset freeze); *FTC v. Am. Tax Relief LLC, et al.*, No. 10-cv-6123 (N.D. Ill. Sept. 24, 2010) (Kocoras, J.) (*ex parte* TRO with asset freeze and appointment of a receiver); *FTC v. Asia Pacific Telecom, Inc., et al.*, No. 10-cv-3168 (N.D. Ill. May 25, 2010) (Hart, J.) (*ex parte* TRO with asset freeze and appointment of receiver); *FTC v. API Trade, LLC, et al.*, No. 10-cv-1543 (N.D. Ill. March 10, 2010) (Guzman, J.) (*ex parte* TRO with asset freeze); *FTC v. 2145183 Ontario Inc., et al.*, No. 09-cv-7423 (N.D. Ill. Nov. 30, 2009) (Grady, J.) (*ex parte* TRO with asset freeze and appointment of receiver).

corporate defendants [are] available to make restitution to the injured consumers.” *Id.* at 1031. In a case such as this, in which the FTC is likely to succeed in showing that officers and managers are individually liable for the payment of restitution, the freeze should extend to individual assets as well. *Id.* (affirming freeze on individual assets); *see also FTC v. Datacom Mktg. Inc.*, No. 06-cv-2574, 2006 WL 1472644, at *5 (N.D. Ill. 2006) (freezing assets of individual and corporate defendants).

2. Temporary Receiver

Plaintiffs seek the appointment of a temporary receiver pursuant to the Court’s equitable powers under Section 13(b) of the FTC Act. Such an appointment is particularly appropriate when, as here, Defendants’ pervasive fraud presents a strong likelihood of continued misconduct. A temporary receiver would prevent the destruction of documents and dissipation of assets as well as secure sensitive consumer data. A receiver could also assist the Court in assessing the extent of Defendants’ fraud, trace the proceeds of that fraud, and make an independent report of Defendants’ current and past activities to the Court.

3. Immediate Access and Limited Expedited Discovery

The proposed TRO grants the temporary receiver and Plaintiffs immediate access to the corporate defendants’ physical business premises to locate and to secure Defendants’ assets and documents pertaining to their business practices. For the same purposes, Plaintiffs seek limited expedited discovery into the nature, location, and extent of these assets and documents, including permission to conduct depositions with 48 hours’ notice and to issue requests for production of documents on five days’ notice.

E. The Temporary Restraining Order Should Be Issued *Ex Parte*

To prevent Defendants from dissipating or concealing their assets, the requested TRO should be issued *ex parte*. An *ex parte* TRO is warranted when the facts show that immediate and irreparable injury, loss, or damage will occur before the defendants can be heard in opposition. *See* Fed. R. Civ. P. 65(b). There is a serious risk that assets and evidence stemming from Defendants' illegal activity will disappear if they receive prior notice. The blatantly deceptive nature of Defendants' scheme presents a serious risk that Defendants will destroy documents and dissipate assets if given advance notice of Plaintiffs' motion.¹²³

V. CONCLUSION

For the reasons set forth above, Plaintiffs respectfully request that the Court enter the proposed TRO to halt Defendants' violations of the FTC Act, the Florida Deceptive and Unfair Trade Practices Act, and the Telemarketing Sales Rule and to help ensure the possibility of effective final relief for consumers.¹²⁴

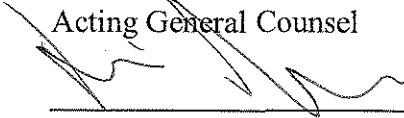
¹²³ *See* Certification and Declaration of FTC Counsel pursuant to Rule 65(b).

¹²⁴ Along with this Memorandum, Plaintiffs have submitted a proposed *Ex Parte* Temporary Restraining Order with Asset Freeze, Appointment of a Receiver, Other Equitable Relief and Order to Show Cause Why a Preliminary Injunction Should Not Issue.

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
Phone: (312) 960-5611 [Davis]
Phone: (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