UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

CASE NO. 14CV81395 MARRA/MATTHEWMAN

FEDERAL TRADE COMMISSION, and

STATE OF FLORIDA,

Plaintiffs,

v.

Inbound Call Experts, LLC also d/b/a Advanced Tech Support, a limited liability company,

Advanced Tech Supportco, LLC, a limited liability company,

PC Vitalware, LLC, a limited liability company,

Super PC Support, LLC, a limited liability company,

Robert D. Deignan, individually and as an officer of Inbound Call Experts, LLC, Advanced Tech Supportco, LLC, PC Vitalware, LLC, and Super PC Support, LLC,

Paul M. Herdsman, individually and as an officer of Inbound Call Experts, LLC, PC Vitalware, LLC, and Super PC Support, LLC,

Justin M. Wright, individually and as an officer of Inbound Call Experts, LLC, PC Vitalware, LLC, and Super PC Support, LLC,

PC Cleaner, Inc., a corporation,

Netcom3 Global, Inc., a corporation,

Netcom3, Inc. also d/b/a Netcom3 Software Inc. and

Cashier Myricks, Jr. a/k/a Cashier Myrick, individually and as an officer of PC Cleaner, Inc., Netcom3 Global, Inc., and Netcom3, Inc.,

Defendants.

Emergency

PLAINTIFFS' *EX PARTE* MOTION FOR A TEMPORARY RESTRAINING ORDER AND MEMORANDUM IN SUPPORT THEREOF

Filed Under Seal

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

FEDERAL AND STATE STATUTES

FEDERAL REGULATIONS

FEDERAL RULES

I. INTRODUCTION

The Federal Trade Commission ("FTC") and the State of Florida, Office of the Attorney General ("State of Florida") respectfully request that the Court halt a technical support scam that has bilked thousands of consumers out of millions of dollars by exploiting their fears about viruses, malware and other security threats on their computers.[1] Defendants Inbound Call Experts, LLC also doing business as Advanced Tech Support ("ICE") and Advanced Tech Supportco, LLC ("ATS") operate enormous call centers that sell technical support services to consumers. Through a variety of ploys to induce consumers to call them, the ICE/ATS[2] inbound telemarketers gain remote access to consumers' computers and then offer to perform a free "diagnostic" check. After showing show consumers a series of screens, Defendants falsely claim that the screens show evidence of infections, past infections, or "trace damages" to consumers' computers. The telemarketers also falsely assert that the purported problems they have identified represent an immediate threat to the computers that can only be resolved manually by a technician.

Once they have duped consumers, many of whom are seniors, into believing that their computers are riddled with problems and in imminent danger of crashing, the ICE/ATS telemarketers pitch the services of the company's technicians. ICE/ATS charges consumers hundreds of dollars for what are often unnecessary repairs, long-term maintenance programs, and installations of free or outdated programs. The company's sales have likely exceeded $100 million since 2013.

---

[1] Plantiffs submit three volumes of exhibits in support of their motion. All exhibits cited in this Memorandum are referenced as "PX [exhibit number]." References to declarations include a relevant paragraph number, and attachments are designated with a relevant page number.
In considering an application for a TRO or preliminary injunction, the Court "may rely on affidavits and hearsay materials" if appropriate. *Levi Strauss & Co. v. Sunrise Int'l Trading, Inc.*, 51 F.3d 982, 985 (11th Cir. 1995).

[2] For the reasons described in Section II below, these entities are collectively referred to as ICE/ATS and treated as a single entity.

As noted above, ICE/ATS relies on a variety of marketing ploys to lure consumers to call its telemarketers. One technique is to partner with multiple computer software developers that agree to direct consumers to call ICE/ATS to activate or register a new software purchase.[3] For example, ICE/ATS partners with Defendant PC Cleaner, Inc. ("PC Cleaner"), which sells a registry cleaning program, PC Cleaner Pro. PC Cleaner Pro instructs consumers who purchase the program to call an ICE/ATS telephone number to activate their new software, thereby generating potential targets for the tech support scam.

PC Cleaner also relies on deception to market its own product. The company advertises free trials of PC Cleaner Pro to identify potential problems with computers. Consumers initially download a free version of PC Cleaner Pro, which then runs a system scan that invariably detects thousands of purported problems in need of repair. PC Cleaner offers consumers the opportunity to "fix" these problems by downloading the paid version of the software for between $29.97 and $39.97. As a final step, PC Cleaner directs purchasers to call ICE/ATS to activate their software, thereby subjecting them to the ICE/ATS sales pitch.

Because Defendants' conduct has already injured tens of thousands of consumers across the country and around the world, and continues to harm additional consumers on a daily basis, Plaintiffs seek an *ex parte* temporary restraining order ("TRO") that will stop Defendants' deceptive business practices and preserve assets for potential redress to consumers. Specifically, Plaintiffs seek an *ex parte* TRO that enjoins Defendants from continuing their illegal practices and orders ancillary equitable relief, including: an asset freeze, the appointment of a temporary receiver, immediate access to relevant business premises and records, limited expedited discovery, and an order to show cause why a preliminary injunction should not issue. These

[3] ICE/ATS also partners with established computer security software companies to have ICE/ATS phone numbers displayed as technical support numbers for various software products.

measures are necessary to prevent continued consumer injury, dissipation of assets, and destruction of evidence, thereby preserving this Court's ability to provide effective final relief to the victims of Defendants' scheme.

II. STATEMENT OF FACTS

Since at least 2011, Defendants have relied on an escalating series of deceptive scare tactics to sell their computer products and services. Defendants' deceptive and misleading sales pitches prey on consumers' fears and inexperience, and Defendants have successfully convinced thousands of consumers to purchase unnecessary, and in some instances harmful, products and services.

A. The PC Cleaner Corporate Defendants' Deceptive Business Practices

The PC Cleaner Corporate Defendants[4] sell a registry cleaner called PC Cleaner Pro, which purports to "Fix, Clean & Speed Up Your PC in Minutes" by correcting information in the Windows registry, cleaning up "unwanted history data," adjusting system settings, "swiftly" removing malware and cleaning out "accumulated system clutter."[5] The product's website offers a "FREE Computer Scan" for consumers who are willing to download a free version of PC Cleaner Pro.[6]

PC Cleaner Pro's free computer scan is a highly deceptive marketing tool used by the PC Cleaner Corporate Defendants to scare consumers into purchasing the paid version of PC

[4] PC Cleaner, Netcom3 Global, Inc. ("Netcom3 Global") and Netcom3, Inc., also doing business as Netcom3 Software, Inc. ("Netcom3") are collectively referred to as the PC Cleaner Corporate Defendants. As alleged in the Complaint and discussed in Section III.B.3 below, these entities operate as a common enterprise.
[5] PX 30 (Declaration of Michael Kraemer ("Kraemer Dec.")) ¶ 40 & Att. M, p. 867. A registry cleaner is a software product designed to identify and resolve problems with the Windows registry, a database that stores configuration settings and options on Microsoft Windows operating systems.
[6] *Id.* *See also* PX 6 (Declaration of Teresa Daniel ("Daniel Dec.")) ¶ 3; PX 13 (Declaration of Thomas Prytko ("Prytko Dec.")) ¶¶ 2-3.

Cleaner Pro, which costs between $29.97 and $39.97.[7] As described below, the scan is designed to identify hundreds, or even thousands of problems on nearly any computer, even a computer that is in perfect operating condition and performing at its ideal capacity.[8]

According to the Plaintiffs' expert, the scan deceptively categorizes many common and innocuous items – including every temporary file and web browsing cookie and even some Windows default settings – as "problems" that require repair.[9] Many applications use temporary files as part of their normal operations, and these files do not imperil the security or performance of a computer.[10] Similarly, web browsing cookies are commonly used for many benign purposes, such as keeping a user logged into an e-mail account, and typically are not a cause for concern.[11] Nonetheless, the PC Cleaner Pro scan counts each individual temp file and cookie as a problem, thus guaranteeing that the scan results will always show a significant number of "problems" in need of attention.

Additionally, the scan is programmed to identify whether the computer being scanned blocks 926 specific pieces of malware.[12] The scan then separately counts as a "problem" each specimen that is not blocked.[13] These particular 926 pieces of malware, however, date back to at least 2004 and have not been active threats in many years. Because these malware specimens have been inactive for so long, Microsoft does not include them as specific blocks in default Windows installations that come pre-installed with Windows Defender, a comprehensive anti-

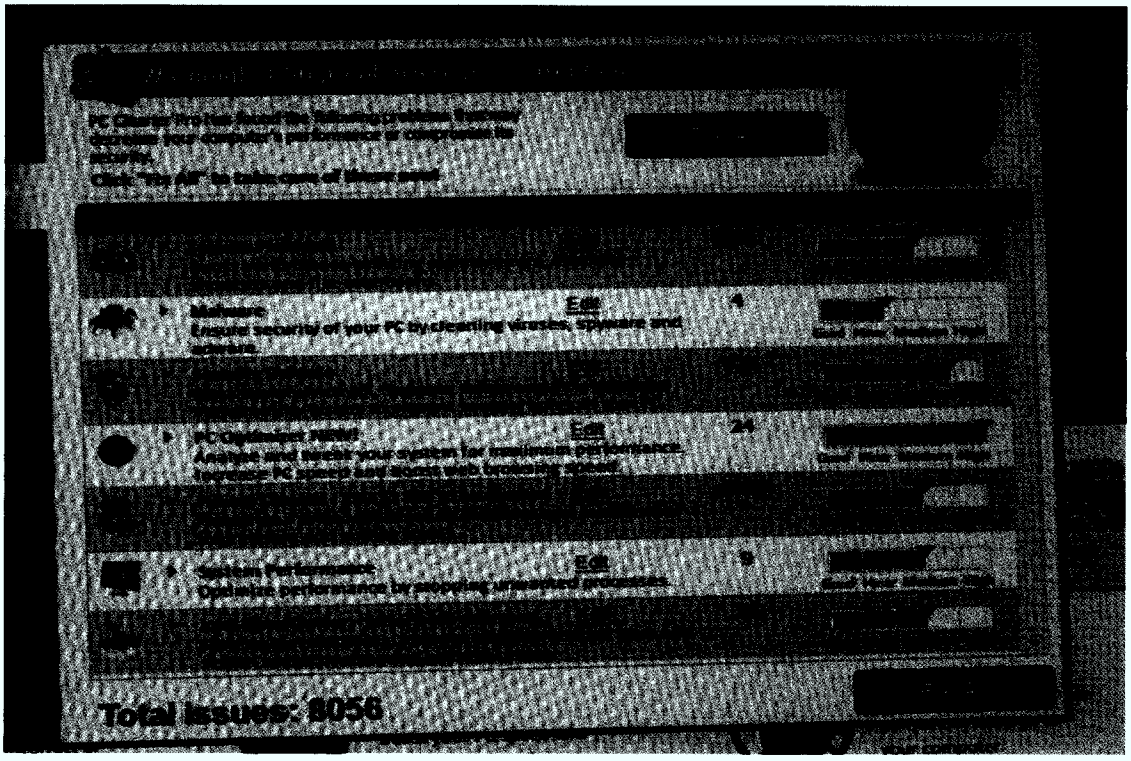
---

[7] PX 30 (Kraemer Dec.) ¶ 14, ¶ 40 & Att. M, p.877; PX 28 (Vera Dec.) ¶ 12, Att. L, p. 365; PX 2 (Declaration of Greg Beltran ("Beltran Dec.")) ¶ 6; PX 6 (Daniel Dec.) ¶¶ 3, 7; PX 13 (Prytko Dec.) ¶¶ 3, 6.
[8] PC Cleaner recently settled a class action suit alleging deceptive marketing of PC Cleaner Pro. PX 29 (Declaration of John Aiken ("Aiken Dec.")) ¶ 61 & Att. AA.
[9] PX 18 (Declaration of Edward F. Skoudis ("Skoudis Dec.")) Att. A, pp. 72-73.
[10] *Id.* at p. 72.
[11] *Id.* at p. 73.
[12] *Id.*
[13] *Id.*

malware program.[14] The result is that almost every computer currently in operation will fail to block these 926 malware specimens, and accordingly, PC Cleaner Pro's scan will always find at least 926 additional "problems" on nearly any computer, even though these specimens are not active and blocking them provides no defense against modern malware.[15]

As part of its investigation into the PC Cleaner Corporate Defendants, the FTC downloaded the free version of PC Cleaner Pro onto completely clean computers with newly-installed operating systems.[16] Each scan identified thousands of privacy and system "problems" and indicated it had found malware on the computer.[17] A screenshot of one of the scan results,[18] showing 8,056 purported security or performance problems (including four instances of malware), on a pristine FTC computer, is below:

[14] *Id.*
[15] *Id.*
[16] PX 23 (Declaration of Tina Del Beccaro ("Del Beccaro Dec.")) ¶ 6; PX 28 (Declaration of Martha W. Vera ("Vera Dec.")) ¶ 8; PX 30 (Kraemer Dec.) ¶¶ 11 &14.
[17] PX 30 (Kraemer Dec.) ¶ 14, Att. A, p. 693; PX 28 (Vera Dec.) ¶ 9, Att. L, p. 364.
[18] PX 28 (Vera Dec.) Att. L, p. 364.



(Image 1)

After the scan identifies numerous "problems that may decrease your computer's performance or compromise its security," consumers are prompted to "[c]lick 'Fix All' to take care of [the problems] now."[19] When consumers click the "Fix All" button, they learn that they must "register" (not purchase) the already-downloaded software. Only then does the website finally disclose that registering the software will cost between $29.97 and $39.97.[20]

Although many consumers are induced to purchase PC Cleaner Pro primarily because the scan overstates and mischaracterizes "problems,"[21] the PC Cleaner Corporate Defendants also misrepresent that the PC Cleaner Pro registry cleaner can fix those problems and otherwise

[19] *See* Image 1. *See also* PX 2 (Beltran Dec.) ¶ 5; PX 6 (Daniel Dec.) ¶ 3; PX 13 (Prytko Dec.) ¶ 3.
[20] PX 28 (Vera Dec.) ¶¶ 10-12 & Att. L, pp. 364-65. *See also* Footnote 7 *supra* regarding range of prices.
[21] *See, e.g.*, PX 13 (Prytko Dec.) ¶ 3 ("The scan told me that I had thousands of errors on my computer. Even though I had only had my computer for about one year and I had Norton [antivirus software] on my computer, the scan results made me nervous that something was wrong with my computer. I decided to pay for the product and fix the errors.").

increase computers' speed and performance. In reality, registry cleaners like PC Cleaner Pro are at best unnecessary and at worst can cause slower start-up times, poor application functionality, and random crashes – the very problems that PC Cleaner Pro claims to solve.[22] More importantly, most consumers download the program to fix the "problems" identified in the scan, and those problems either do not exist[23] or do not affect the performance or security of the computer.[24] In short, the PC Cleaner Corporate Defendants use the scan's deceptive results to scare consumers into purchasing a largely unnecessary and potentially harmful software product.

B. The ICE Corporate Defendants' Deceptive Business Practices

Consumers who purchase PC Cleaner Pro and similar products have already been deceived into believing that their computers have significant damage. Further, they have already spent money for a product they likely did not need. The tech support scam, however, has only just begun. After entering their credit card information to pay for PC Cleaner Pro (or another product the ICE Corporate Defendants[25] use as a lead generator), consumers are directed to call a number to "activate" the software.[26] A screenshot of a sample activation page is below:

---

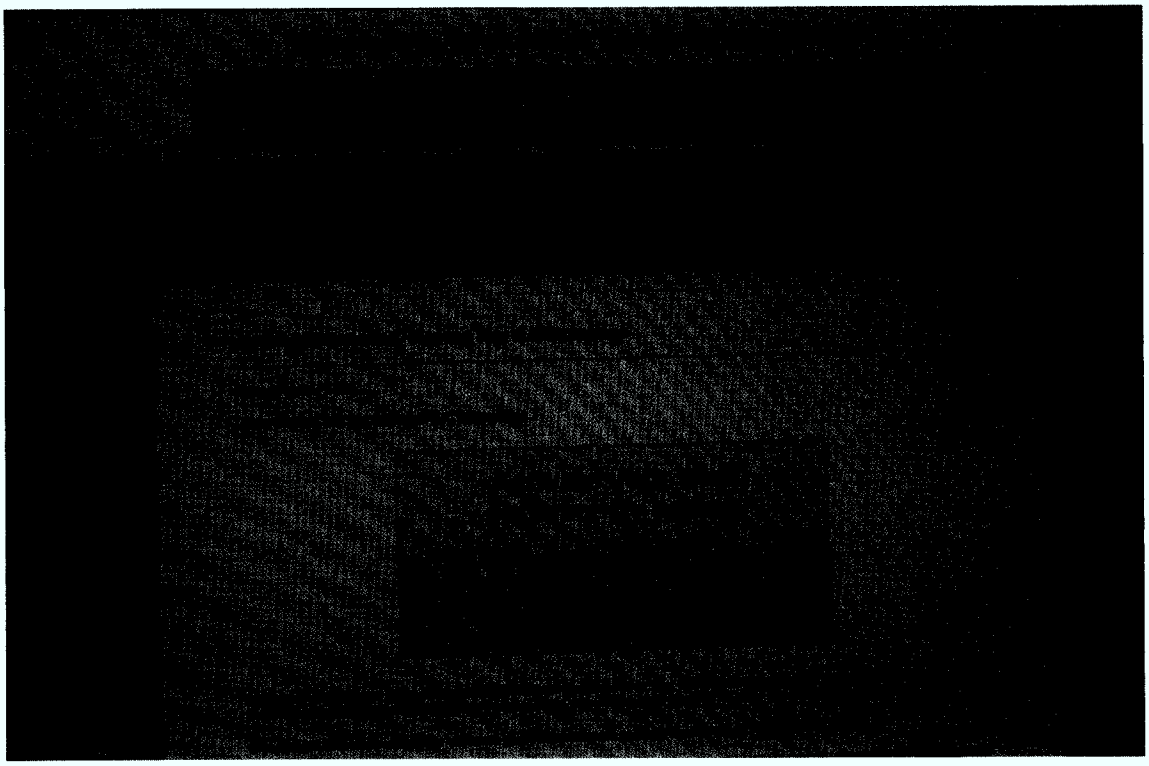
[22] According to Microsoft and the FTC's expert, registry cleaners like PC Cleaner Pro are usually unnecessary, and they can cause serious problems with the Windows operating system. PX 18 (Skoudis Dec.) Att. A, pp. 69-71. Some consumers reported serious problems with their computers after downloading PC Cleaner Pro, including system crashes, malware problems, additional slowness or even complete loss of functionality. *See, e.g.*, PX 2 (Beltran Dec.) ¶¶ 8, 14; PX 13 (Prytko Dec.) ¶¶ 4 & 6; PX 29 (Aiken Dec.) ¶ 80. Consumers who experienced these problems often had to hire real technicians to reverse the damage done by PC Cleaner Pro. *See, e.g.*, PX 13 (Prytko Dec.) ¶ 10.

[23] For example, the PC Cleaner Pro scan of the FTC's computers detected malware that simply did not exist. PX 18 (Skoudis Dec.) Att. A, p. 65 ("The initial machines were clean and uninfected by malware.").

[24] *See* PX 18 (Skoudis Dec.) Att. A, pp. 72-73.

[25] ICE, ATS, PC Vitalware, LLC and Super PC Support, LLC are collectively referred to as the ICE Corporate Defendants. As alleged in the Complaint and discussed in Section III.B.3 below, these entities operate as a common enterprise.

[26] PX 30 (Kraemer Dec.) ¶ 14 & Att. A, p. 694; PX 28 (Vera Dec.) ¶ 13 & Att. L, p. 368.



(Image 2)

ICE/ATS leases at least 240 toll-free telephone numbers, and the company displays these numbers in a variety of contexts.[27] Many of the ICE/ATS phone numbers appear on activation pages, like the one shown above, for particular software products,[28] but consumers also may encounter ICE/ATS telephone numbers through Internet advertisements, Google search results, or other sources.[29] When consumers call any of these phone numbers, they are connected directly to an ICE/ATS telemarketer, who offers to register software or otherwise assist them.

---

[27] PX 29 (Aiken Dec.) ¶ 39.

[28] A list of other software products known to serve as lead generators for ICE/ATS is included as Attachment EE to PX 29 (Aiken Dec.) ¶¶ 73-74. *See also* PX 1 (Declaration of James Barnes ("Barnes Dec.")) ¶¶ 1-2; PX 3 (Declaration of Judy Marie Callahan ("Callahan Dec.")) ¶ 4; PX 8 (Declaration of Robert Ernst ("Ernst Dec.")) ¶ 3; PX 11 (Declaration of Richard Heupel ("Heupel Dec.")) ¶ 2; PX 12 (Declaration of Donald Holmes ("Holmes Dec.")) ¶¶ 3 & 4; PX 13 (Prytko Dec.) ¶ 3; PX 14 (Declaration of Donna Reddin ("Reddin Dec.")) ¶ 4; PX 15 (Declaration of Debbie Rhodes ("Rhodes Dec.")) ¶ 4.

[29] *See* PX 29 (Aiken Dec.) ¶¶ 63-69; PX 4 (Declaration of Susan Carr ("Carr Dec.")) ¶ 2; PX 5 (Declaration of Barbara Cheatham ("Cheatham Dec.") ¶¶ 1-2; PX 7 (Declaration of Ophelia Dees ("Dees Dec.")) ¶ 2; PX 9 (Declaration of Gary Green ("Green Dec.")) ¶ 1; PX 10 (Declaration of Barbara Harris ("Harris Dec.")) ¶ 3. The FTC's investigation revealed that the ICE Corporate Defendants also generated leads for the ICE/ATS call center by

Before doing so, the telemarketers walk consumers through a process that allows the telemarketers to remotely access consumers' computers.[30] Remote access gives telemarketers control over the computers – they can move cursors, enter commands, run applications, and access stored information. This control amplifies the sales pitch by adding a visual element – consumers might be more likely to trust representations that appear to be supported by something they can see on their own computer screens.

Soon after gaining access, the ICE/ATS telemarketers offer to "perform a quick diagnosis to make sure everything is working properly."[31] Then they launch into a lengthy "diagnostic" that includes, among other things, evaluating the Microsoft System Configuration (msconfig)[32] window and the Event Viewer.[33] In reality, however, this process is not a diagnostic test designed to identify the source of computer problems. Rather, it is a scripted sales pitch that inevitably leads to the conclusion that consumers' computers are severely compromised and in need of immediate repair.[34]

---

partnering with well-known security companies like Panda Security to purportedly provide customer support for specific products. For example, the telephone number that appears on Panda Security's website for "Free US Based telephone support" is a number owned by the ICE Corporate Defendants. During an undercover call to that number, an FTC investigator said that her Panda software was not opening. A telemarketer remotely connected to her computer, but did not try to open the Panda software, let alone fix it. Rather, he launched into the scripted sales pitch described below in this Section. *See* PX 28 (Vera Dec.) ¶¶ 24-35.

[30] ICE/Vast telemarketers originally directed consumers to the website of LogMeIn, a third-party remote access software program, at which point consumers would be directed to enter a code to cede control to the telemarketers. PX 29 (Aiken Dec.) ¶¶ 51-52. More recently, the company now appears to use a program called Nexus for this purpose. PX 29 (Aiken Dec.) ¶ 51, n.16; PX 30 (Kraemer Dec.) ¶ 15.

[31] PX 30 (Kraemer Dec.) Att. Y, p. 968 (telemarketing script). *See also* PX 28 (Vera Dec.) Att. A, p. 193.

[32] Microsoft System Configuration ("msconfig") is a built-in Windows utility that allows users to view, disable, or re-enable some programs that automatically load on startup. PX 18 (Skoudis Dec.) Att. A, p. 64.

[33] PX 30 (Kraemer Dec.) ¶¶ 16-17, Att. B, pp. 710-12, Att. Y, p. 969-71; PX 28 (Vera Dec.) ¶¶ 16-17, Att. A. pp. 195-97.

[34] PX 18 (Skoudis Dec.) Att. A, p. 65. For example, during one portion of the "diagnostic," telemarketers open the msconfig start-up tab, which shows how many programs are set to load when the computer starts. Telemarketers warn consumers that their computers will run more slowly if too many programs load at start-up. Then the script instructs telemarketers to say without any analysis: "Just taking a quick glance I notice a lot of unnecessary programs that do not need to start." PX 30 (Kraemer Dec.) Att. Y, p. 970. *See also* PX 9 (Green Dec.) ¶ 2.

1. Misrepresentations Regarding "Running Services" and "Trace Elements" in the Microsoft System Configuration (msconfig)

Early on in the purported diagnosis process, the ICE/ATS telemarketers open msconfig, and tell consumers that most software leaves behind "running services" and "trace elements."[35] They then assert that these purported "trace elements" can build up over time and cause the computer to crash, leading to the "dreaded blue screen."[36] According to the FTC's expert, these statements are "flagrantly false."[37] In reality, the vast majority of uninstallation packages fully remove the associated software without leaving anything behind – exactly the opposite of the telemarketers' representations.[38] Moreover, "running services" and "trace elements" (which is not an industry term) typically have no correlation with the speed or performance of a computer.[39] In general, even if anything had been left behind, the computer would be no worse off after uninstalling software than it would be if the software remained installed.[40] In addition, "running services" have no relation to the ability to install or uninstall software or to crashes and "blue screens."[41]

Notably, the computers used for the FTC's undercover calls had very few pieces of software installed, and according to the FTC's expert, the computers had no running services and nothing otherwise anomalous or suspicious.[42] Nonetheless, in each undercover call, the ICE/ATS telemarketer raised concerns about "running services" and "trace elements" and

---

[35] PX 30 (Kraemer Dec.) Att. B, p. 710 & Att. Y, p. 970; PX 28 (Vera Dec.) Att. A, p. 196 & Att. D, pp. 275-76.
[36] *Id.*
[37] PX 18 (Skoudis Dec.) Att. A, p. 81.
[38] *Id.*
[39] *Id.* at p. 80-81.
[40] *Id.* at p. 81.
[41] *Id.*
[42] *Id.* at p. 76.

alleged that catastrophic consequences would result if these were not cleaned up by a "certified technician."[43]

2. Misrepresentations Regarding "Damage" and "Trace Damage" in the Windows Event Viewer[44]

For the final step of the diagnosis, the ICE/ATS telemarketers direct consumers to the Window Event Viewer.[45] According to the telemarketers, this "last and most important step" is necessary for "checking the overall health of your computer."[46] After opening the Event Viewer, telemarketers show consumers a long list of errors (designated in red) and warnings (designated in yellow).[47] A sample screen shot of an Event Viewer log appears below:

[43] PX 30 (Kraemer Dec.) ¶ 16, Att. B, p. 710; PX 28 (Vera Dec.) ¶¶ 16-18, Att. A, p. 196.
[44] Interestingly, the written script includes the following warning: "**DO NOT SAY EVENT VIEWER!!!**" PX 30 (Kraemer Dec.) Att. Y, p. 971 (emphasis in original). A former employee confirmed that telemarketers were instructed never to use the phrase "Event Viewer" during this portion of the sales pitch and in fact they could be fired if they used that term. PX 30 (Kraemer Dec.) ¶ 55. This strict policy against saying "Event Viewer" may have been formulated in response to a group of FTC cases brought against companies, primarily in India, operating similar tech support scams. Telemarketers in those cases relied heavily on the Event Viewer to scare consumers into purchasing products and services. *See* http://www.ftc.gov/news-events/press-releases/2012/10/ftc-halts-massive-tech-support-scams.
[45] *See, e.g.*, PX 9 (Green Dec.) ¶ 2; PX 10 (Harris Dec.) ¶ 4; PX 11 (Heupel Dec.) ¶ 3; PX 12 (Holmes Dec.) ¶ 7; PX 13 (Prytko Dec.) ¶ 4; PX 14 (Reddin Dec.) ¶ 5; PX 15 (Rhodes Dec.) ¶ 6.
[46] PX 30 (Kraemer Dec.) ¶ 17, Att. B, p. 711, Att. Y, p. 971; PX 28 (Vera Dec.) Att. A, p. 197.
[47] Although the Event Viewer log typically shows many more innocuous-looking entries (like a white and blue "information" entry), the ICE/ATS telemarketers were instructed to filter the log so that it only showed errors and warnings. PX 16 (Tomich Dec.) ¶ 9.

Application Number of events: 5,801

Filtered: Log: Application; Levels: Critical, Error, Warning; Source: . Number of events: 495

Level	Date and Time	Source	Event ID	Task C...
Warning	11/5/2014 10:56:18 AM	User Profile Service	1530	None
Warning	11/4/2014 1:04:01 PM	Group Policy Drive Maps	4098	(2)
Warning	11/3/2014 10:43:55 PM	User Profile Service	1530	None
Warning	11/3/2014 10:43:22 PM	MsiInstaller	1001	None
Warning	11/3/2014 10:43:22 PM	MsiInstaller	1004	None
Error	11/3/2014 3:16:14 PM	Application Error	1000	(100)
Error	11/3/2014 3:00:26 PM	Application Error	1000	(100)
Warning	11/3/2014 11:34:36 AM	MsiInstaller	1001	None
Warning	11/3/2014 11:34:36 AM	MsiInstaller	1004	None
Error	10/31/2014 11:55:17 PM	SideBySide	80	None
Warning	10/31/2014 3:22:06 PM	MsiInstaller	1001	None
Warning	10/31/2014 3:22:06 PM	MsiInstaller	1004	None
Warning	10/31/2014 2:05:38 PM	User Profile Service	1530	None
Warning	10/30/2014 2:37:20 PM	User Profile Service	1530	None
Warning	10/30/2014 11:01:46 AM	Group Policy Drive Maps	4098	(2)
Warning	10/28/2014 2:49:02 PM	Symantec AntiVirus	129	None
Warning	10/28/2014 2:00:53 PM	Symantec AntiVirus	129	None
Warning	10/28/2014 1:20:19 PM	Group Policy Drive Maps	4098	(2)
Error	10/28/2014 1:23:07 AM	SideBySide	80	None
Error	10/24/2014 7:56:49 AM	Symantec AntiVirus	51	None
Error	10/22/2014 1:22:16 AM	SideBySide	80	None
Warning	10/21/2014 5:47:08 PM	Symantec AntiVirus	129	None
Warning	10/21/2014 4:29:36 PM	Group Policy Drive Maps	4098	(2)
Warning	10/21/2014 11:28:33 AM	Symantec AntiVirus	129	None
Warning	10/21/2014 10:39:35 AM	User Profile Service	1530	None
Warning	10/21/2014 10:09:25 AM	User Profile Service	1530	None

(Image 3)

The ICE/ATS telemarketers falsely assert that these red and yellow designations are signs of significant damage or threats that severely compromise the security or performance of consumers' computers.[48] According to a former ICE/ATS employee, this portion of the sales pitch is designed to scare consumers and close the sale.[49] Indeed, many consumers who complained to the FTC reported feeling particularly alarmed during this portion of the sales call. According to one consumer: "[H]e brought up a screen on my machine that showed me errors

[48] According to the script: "Every one of these errors and warnings are a red flag. It's normal to have a few --- '**but look how many there are**'. There's a significant amount of damage on this computer." (emphasis and punctuation in original). PX 30 (Kraemer Dec.) Att. Y, p. 971. *See also* PX 9 (Green Dec.) ¶ 2 ("He showed me something called the event viewer that showed many unresolved issues."); PX 10 (Harris Dec.) ¶ 4 ("[H]e brought up a screen on my machine that showed me errors and warnings on the computer. It looked very scary. I believe there were red x's and yellow triangles and a list of errors."); PX 12 (Holmes Dec.) ¶ 7 ("Then, Mike pulled up something on my computer screen that I had never seen before. He showed me pages and pages of warnings and errors. I noticed that the pages on my screen were from a window called the "event viewer." He told me these warnings and errors needed to be fixed."); PX 13 (Prytko Dec.) ¶ 4 ("Among other things, he showed me the event viewer screen on my computer and it showed that there were lots of red x's and yellow triangles. The telemarketer said that this meant my computer was corrupt."); PX 14 (Reddin Dec.) ¶ 5 ("[S]he pulled up a screen that showed a list of errors. When she pulled up that screen she said 'wow' and told me I had a lot of errors on my computer. That made me very scared because I did not realize I had errors on my computer."); PX 15 (Rhodes Dec.) ¶ 6 ("Then he showed me a screen with lots of red x's and yellow triangles and told me that this showed there were threats on my computer.").

[49] PX 16 (Tomich Dec.) ¶ 9.

and warnings on the computer. It looked very scary. I believe there were red x's and yellow triangles and a list of errors."[50] Another consumer stated: "[S]he pulled up a screen that showed a list of errors. When she pulled up that screen she said 'wow' and told me I had a lot of errors on my computer. That made me very scared because I did not realize I had errors on my computer."[51]

After opening the Event Viewer log, the ICE/ATS telemarketers explain that "the way that this [the errors and warnings in log] occurs in most cases is infections or past infections on the computer, it's called what's known as trace damage."[52] They then ask whether consumers have security protection software. If consumers say they do not have security software, the telemarketers say that the purported "damage" shown in the Event Viewer is a result of "not having quality protection software."[53] If consumers say they do have security software, the telemarketers say that the security software itself is leaving behind "trace damage" that builds up over time.[54] Either way, the script leads to the inevitable conclusion that every computer is damaged and in need of repair.

In reality, there is no correlation between what appears in the Event Viewer and the overall health of a computer.[55] The Event Viewer is a Windows utility that logs and displays information about prior events within the operating system. Events are categorized in a number of ways, including "errors" and "warnings," but neither the number of events nor the way they are categorized is necessarily indicative of any serious issues.[56] In fact, errors and warnings are commonly reported as part of the operating systems' normal day-to-day operations and are not

---

[50] PX 10 (Harris Dec.) ¶ 4.
[51] PX 14 (Reddin Dec.) ¶ 5.
[52] PX 30 (Kraemer Dec.) ¶ 17 & Att. B, pp. 711-12, Att. Y, p. 970; PX 28 (Vera Dec.) ¶ 17, Att. A, pp. 198-99.
[53] PX 30 (Kraemer Dec.) Att. Y, p. 972. *See also* Att. B, pp. 711-12.
[54] *Id.* at Att. Y, p. 972; PX 28 (Vera Dec.) Att. A, p. 200.
[55] PX 18 (Skoudis Dec.) Att. A, p. 81.
[56] *Id.* at p. 81.

indicative of damage or even of "trace damage."[57] According to the FTC's expert, seeing a Windows Installation without warnings and errors would be an extremely unusual occurrence.[58] Therefore, it is highly misleading to describe these innocuous entries in a log as "damage" or to state that a computer might crash simply because of the number of entries in the log.[59] These statements are clearly designed to scare consumers into purchasing technical support services even though the ICE/ATS telemarketers have no reason to know whether they are necessary.

3. Finalizing the Sale of Tech Support Services and Upsell of Additional Security Software

Having convinced consumers that their Event Viewer logs show evidence of significant damage, the ICE/ATS telemarketers then pitch their company's services. They state that only a "certified technician" performing manual work can repair the "damages" shown in the logs, and warn that if left unrepaired, the damages "CAN cause your computer to crash."[60] Then they offer the services of their "Microsoft-certified technicians" who will fix the purported damage remotely for between $250 and $400, sometimes with a recurring monthly fee of $14.95 or more.[61] Before finalizing the sale, the script requires telemarketers to ask about "protection software" and pitch one of their partners' products, such as Panda Security or Malwarebytes at

---

[57] *Id.* at pp. 76, 81.
[58] *Id.* at p. 76.
[59] *Id.* at p. 67.
[60] PX 30 (Kraemer Dec.) ¶ 17, Att. B, p. 713, Att. Y, p. 972; PX 28 (Vera Dec.) ¶ 18, Att. A, p. 201. These statements are false. In reality, anyone can remove the errors and warnings from the Event Viewer simply by deleting them. Notably, the only thing the ICE/ATS "technicians" do to address the errors and warnings in the Event Viewer is delete the log files. PX 18 (Skoudis Dec.) Att. A, p. 77. Further, according to the FTC's expert, if there were software problems on a computer, software could be used to correct those problems without a technician. *Id.* at p. 82. Most importantly, the error and warning entries in the Event Viewer log are not "damage" nor evidence of damage, and there is no correlation between these entries and the likelihood that a computer will crash. *Id.* at pp. 67 & 81.
[61] PX 7 (Dees Dec.) ¶ 3 (paid $180 and $14.95 monthly); PX 8 (Ernst Dec.) ¶ 6 (paid $205 and $19.99 monthly); PX 10(Harris Dec.) (paid $180 and $14.99 monthly); PX 14 (Reddin Dec.) (paid $205 and $14.99 monthly); PX 16 (Tomich Dec.) ¶ 10 (packages range between $150 and $250 with monthly fees ranging from $14.99 to $29.99); PX 28 (Vera Dec.) ¶ 19, Att. A, p. 202; PX 30 (Kraemer Dec.) ¶ 18, Att. B, p. 716, Att. Y, p. 973.

exorbitant prices.[62] Even if consumers already had security software on their computers, the telemarketers were instructed to push the upsell by telling consumers that their existing software was inadequate.[63] Finally, the telemarketers charge consumers' credit cards, and transfer their remote access sessions to the ICE/ATS "technicians" for purported clean-up and maintenance.[64]

4. Purported Clean-Up and Maintenance

The Plaintiffs' expert analyzed memory captures and hard drive images taken from the FTC computers after the ICE/ATS technicians completed their work to determine what the technicians had done to purportedly "fix" the computer.[65] According to the expert, the technicians: (1) manually deleted the log files in the Event Viewer program to make it appear as though the purported "damages," *i.e.*, the red and yellow error and warning entries in the log, had been repaired; (2) installed a series of cleanup and backup utilities and accepted the licenses of these tools (without the FTC's consent); and (3) installed an emergency recovery utility that is **not** compatible with Windows 7, the operating system the FTC installed on the undercover computer.[66] The technicians did not remove the remote support utilities that had been downloaded to permit remote access.

---

[62] PX 1 (Barnes Dec.) ¶6; PX 5 (Cheatham Dec.) ¶ 3; PX 7 (Dees Dec.) ¶ 4; PX 8 (Ernst Dec.) ¶ 5; PX 9 (Green Dec.) ¶ 3; PX 10 (Harris Dec.) ¶ 5; PX 11 (Heupel Dec.) ¶ 3; PX 30 (Kraemer Dec.) ¶ 19, Att. B, pp. 725-726, Att. Y, p. 974; PX 28 (Vera Dec.) ¶ 20, Att. A, p. 217. For example, in one of the FTC's undercover calls, the telemarketer pitched a "lifetime" version of Panda Security software for $500. PX 30 (Kraemer Dec.) ¶ 19, Att. B, pp. 725-726. Panda Software is available at www.panda.com. The longest license available on the website is for three years, and the cost for one computer is approximately $82.00. A former employee said that ATS created a website for the anti-virus software showing an inflated MSRP of $500 and would show it to customers to try to get them to pay that amount. PX 16 (Tomich Dec.) ¶ 11.

[63] PX 9 (Green Dec.) ¶ 3; PX 10 (Harris Dec.) ¶ 5; PX 16 (Tomich Dec.) ¶ 11; PX 28 (Vera Dec.) Att. A, pp. 217-218.

[64] PX 2 (Beltran Dec.) ¶ 7; PX 3 (Callahan Dec.) ¶ 7; PX 5 (Cheatham Dec.) ¶ 4; PX 7 (Dees Dec.) ¶ 5; PX 8 (Ernst Dec.) ¶7; PX 10 (Harris Dec.) ¶ 6; PX 11 (Heupel Dec.) ¶ 5; PX 13 (Prytko Dec.) ¶ 5; PX 14 (Reddin Dec.) ¶¶ 7-8; PX 15 (Rhodes Dec.) ¶8.

[65] PX 18 (Skoudis Dec.) Att. A, p. 68.

[66] *Id.* at pp. 77-79, 83-84.

None of this work was necessary, since the undercover computer was already in pristine condition.[67] Moreover, the FTC expert concluded that although the cleanup utilities might slightly improve the performance of the computer, the remote support utility left behind might actually slow the computer's performance.[68] In other words, for $250.00 the ICE Corporate Defendants did nothing to improve an already pristine computer, and may in fact have made it worse.

C. The Role of the Defendants

1. PC Cleaner Corporate Defendants

PC Cleaner, Netcom3 Global, Inc. ("Netcom3 Global") and Netcom3, Inc., also doing business as Netcom3 Software, Inc. ("Netcom3"), are all California corporations with their principal places of business in California.[69] The addresses listed on their corporate documents are rented mailboxes, however, so any actual business operations likely occur elsewhere in California.[70] The PC Cleaner Corporate Defendants sell a software product, PC Cleaner Pro, that purports to be a registry cleaner.[71] The product is marketed through the PC Cleaner Corporate Defendants' websites, as well as through pop-up advertisements and search engine results.[72] The PC Cleaner Corporate Defendants also generate inbound calls for ICE/ATS by directing purchasers of PC Cleaner Pro to call an ICE/ATS number in order to activate the software.[73]

---

[67] *Id.* at pp. 68 & 79.
[68] *Id.* at p. 79.
[69] PX 29 (Aiken Dec.) ¶¶ 24-26.
[70] *Id.* at ¶¶ 109-11.
[71] *Id.* at ¶¶ 70-71.
[72] *Id.* at ¶¶ 70-72.
[73] *Id.* at ¶¶ 72-73.

2. PC Cleaner Individual Defendant

Cashier Myricks, Jr. aka Cashier Myrick is the principal of PC Cleaner, Netcom3 Global and Netcom3.[74] He registered the domains pc-cleaners.com and netcom3global.com and is listed as the President of Netcom3 on a related website, netcom3-pccleaner.com.[75] Myricks opened two of the three rented postal boxes that he uses as business addresses for the PC Cleaner Corporate Defendants, and he likely controls the third as well.[76] He is also aware that consumers are unhappy with his deceptive sales tactics for PC Cleaner Pro. In May 2012, consumers brought a class action lawsuit against PC Cleaner alleging that the PC Cleaner Pro free trial version and scan misrepresented that there were errors and problems on consumers computers.[77] Myricks was not named personally in the class action,[78] but he was involved in the litigation, which the company recently settled.[79]

3. ICE Corporate Defendants

ICE is a Florida limited liability company with its principal place of business in Boca Raton, Florida.[80] The company was formed in 2011, and now has more than 800 employees engaged in selling remote technical support services and related products to consumers throughout the United States, Canada, the United Kingdom and Australia.[81] It operates 24 hours

---

[74] *Id.* at ¶ 30.
[75] PX 30 (Kraemer Dec.) ¶ 45, 48.
[76] PX 29 (Aiken Dec.) ¶¶ 109-11.
[77] *Kulesa v. PC Cleaner, Inc.*, Case No. 8:12-cv-00725 (C.D. Cal. May 4, 2012). *See also* PX 29 (Aiken Dec) ¶ 61.
[78] Myricks was named, however, when the FTC sued him for deceptive acts or practices in connection with the advertising, marketing and sale of a peer-to-peer file sharing program referral and tutorial service. *FTC v. Cashier Myricks, Jr. dba MP3downloadcity.com*, Case No. cv 05-7013 (C.D. Cal. Sept. 27, 2005). Myricks settled the FTC action. That settlement permanently enjoined him from, among other things, "misrepresenting, expressly or by implication, any fact material to a consumer's decision to buy or accept any good or service." *See* PX 29 (Aiken Dec) ¶ 62 & Att. DD.
[79] *Id.* at ¶ 61 & Att. AA. The settlement was approved on August 26, 2014. It requires PC Cleaner to make specific modifications to its software and provide each class member with three months of free access to an upgrade, PC Antivirus Pro 2013. It also requires PC Cleaner to pay $316,015.02 for plaintiffs' attorney's fees, $2,000 as an incentive award to the class representative, and $10.00 to each class member who submits a valid claim for payment.
[80] *Id.* at ¶ 20.
[81] *Id.* at ¶ 20; PX 30 (Kraemer Dec.) ¶ 61 & Att. F, p. 761.

a day, seven days week, and sells millions of dollars of products and services each month using the deceptive tactics described in detail below.[82]

ATS is a Florida limited liability company with its principal place of business in Boca Raton, Florida.[83] Although separately incorporated, ATS appears to operate entirely as a dba for ICE. ICE registered the fictitious name "Advanced Tech Support," and there is no indication that that ATS has any business operations separate from ICE.[84] Moreover, ICE and ATS share the same office space, officers and employees.[85]

PC Vitalware, LLC ("PC Vitalware") is a Florida limited liability company with its principal place of business in Lighthouse Point, Florida.[86] It is managed by the same individual defendants behind ICE and ATS, and it operates out of the same location as ATS.[87] PC Vitalware produces PCMRI software, which is one of the products that ICE/ATS telemarketers upsell to consumers.[88]

Super PC Support, LLC ("Super PC Support") is a Florida limited liability company with its principal place of business in Boca Raton, Florida.[89] Like PC Vitalware, it is managed by the individual defendants who operate ICE and ATS.[90] Super PC Support also shares a business address with ICE.[91] Super PC Support's website offers a "free Virus Diagnosis and PC Health Check," and advertises a "limited time only special offer" to remove infections from consumers'

---

[82] PX 29 (Aiken Dec.) Att. GG, p. 623; PX 27 (Declaration of Emil George ("George Dec.")) ¶ 10.
[83] PX 29 (Aiken Dec.) ¶ 19.
[84] *Id.* at ¶ 20. For example: (1) in communications with the BBB, the companies are referenced as "Inbound Call Experts d/b/a Advanced Tech Support;" (2) ICE hires the telemarketers, but the telemarketers tell consumers they work for ATS; and (3) the address listed on ATS's corporate filings is a large warehouse facility marked with company logos for both ICE and ATS. *Id.* at Att. GG, p. 624; PX 16 (Tomich Dec.) ¶ 5; PX 21 (Declaration of John Konopka ("Konopka Dec.") ¶ 5.
[85] PX 29 (Aiken Dec.) ¶¶ 19-20, 27-29.
[86] *Id.* at ¶ 21.
[87] PX 29 (Aiken Dec.) Att. D, p. 450; PX 30 (Kraemer Dec.) ¶ 49.
[88] PX 30 (Kraemer Dec.) ¶ 36; PX 1 (Barnes Dec.) ¶ 6; PX 6 (Ernst Dec.) ¶ 5.
[89] PX 29 (Aiken Dec.) ¶ 22.
[90] *Id.*
[91] *Id.*

computers through remote technical services. The website directs consumers to call a phone number owned by ICE that connects consumers to the ICE/ATS telemarketers.[92]

4. ICE Individual Defendants

Robert D. Deignan ("Deignan") is the co-founder and CEO of ICE, the CEO of Super PC Support, and a manager of ATS and PC Vitalware.[93] He is actively involved in the operations of these entities. For example, Deignan is a named subscriber for the hundreds of phone numbers owned by ICE, and he used his business credit card to pay for phone numbers and domains used by the ICE Corporate Defendants.[94] He also paid LogMeIn, a third-party remote access software company that ICE/ATS telemarketers used to access consumers' computers during their sales pitch.[95] In the past two years alone, Deignan has used his business credit card to pay over $2.2 million in business expenses for the ICE Corporate Defendants.[96] When the Better Business Bureau ("BBB") revoked ATS's accreditation, Deignan represented the company in an attempt to get the company reinstated.[97] He was fully aware of the complaints against the company – he reviewed and responded to them over the course of several years – and had ongoing interactions with the BBB throughout the relevant period.[98]

Paul M. Herdsman ("Herdsman") is the Chief Operating Officer of ICE and Super PC Support, and a manager of PC Vitalware.[99] Like Deignan, he is very involved in the operations of the ICE Corporate Defendants. He was the account holder of record for ICE's LogMeIn account between October 2011 and May 2014 and paid for sub-accounts used by ICE/ATS

---

[92] PX 30 (Kraemer Dec.) ¶¶ 30-31.
[93] PX 29 (Aiken Dec.) ¶ 21.
[94] *Id.* at ¶¶ 27, 39.
[95] *Id.* at p. 409, n.15.
[96] *Id.* at ¶ 41.
[97] *Id.* at ¶ 88.
[98] *Id.*
[99] *Id.* at ¶ 28.

telemarketers.[100] He subscribed and paid for telephone numbers used by the ICE Corporate Defendants. He also made payments to anti-virus software vendors whose products were sold by ICE/ATS, and paid for online advertisements soliciting new sales employees.[101] Since 2012, he has used his business credit cart to charge more than $1.7 million in business expenses on his corporate credit card.[102]

Justin M. Wright is the President of ICE and Super PC Support and a manager of PC Vitalware.[103] Like his two business partners, Deignan and Herdsman, he used his corporate account to pay a substantial portion of the companies' business expenses – over $400,000 since 2012, including payments to Google AdWords, to ensure that the ICE Corporate Defendants' websites would be advertised when consumers searched for specified terms.[104] Wright also paid for online advertisements used to solicit new employees and made payments to software vendors.[105]

In addition to paying numerous business expenses with his corporate credit card, Wright knew about complaints regarding the ICE Corporate Defendants' business practices. In October 2013, Wright contacted ThreatTrack Security, an anti-virus company whose product, VIPRE, blocks "bad domains." ThreatTrack had recently blocked the ICE/ATS primary domain, advancedtechsupport.com, due to a significant number of consumer complaints and the BBB's revocation of the company's accreditation.[106] Wright exchanged numerous emails with a malware researcher at ThreatTrack in an attempt to remove the ICE/ATS domain from the

---

[100] *Id.* at ¶ 28 & p. 409, n. 15. LogMeIn is a third-party remote access software provider. The ICE Defendants used this software to remotely connect to consumers' computers. *Id.* at ¶¶ 51-52.
[101] *Id.* at ¶¶ 28 & 42.
[102] *Id.* at ¶ 41.
[103] *Id.* at ¶ 29.
[104] *Id.* at ¶¶ 41-42.
[105] *Id.*
[106] PX 17 (Declaration of Eric Howes ("Howes Dec.")) ¶¶ 2-3.

blocked list.[107] The researcher informed Wright about complaints against the company and supplied him with links to these complaints.[108] Specifically, the researcher informed Wright "that your company's representatives used baseless scaremongering tactics (*e.g.*, remotely connecting to user's PCs and showing them routine errors in the Windows Event Viewer) in order to pressure them into buying unnecessary and outrageously expensive (most quoted prices fall in the $200-$500 range) remediation services and products." The researcher concluded: "These kinds of tactics are indefensible, and we are well within our rights to provide protection to our customers."[109]

D. Consumer Injury

Defendants have used their scare tactics to bilk consumers for more than $100 million since 2011. According to ICE's bank records, the ICE Defendants raked in more than $113 million from their deceptive scheme between September 2011 and August 2014, and they continue to charge additional consumers every day.[110] This money came through Revenuewire, a company in Canada, that acts as ICE's payment processor. All of the Defendants' transactions are processed through an entity owned by Revenuewire called Safecart.[111] The PC Cleaner Defendants have added substantially to the total consumer injury figure. Although we do not have specific numbers for PC Cleaner's total sales, Myricks disclosed in connection with the class action against PC Cleaner that PC Cleaner Pro had been downloaded more than 450,000 times between 2011 and 2013.[112]

---

[107] *Id.* at ¶ 3.
[108] *Id.* at Att. A, p. 59.
[109] *Id.* at Att. A, p. 56.
[110] PX 27 (George Dec.) ¶ 10.
[111] PX 29 (Aiken Dec.) p. 426, n.32 & ¶ 107. Safecart is the billing descriptor that appears on consumers' credit card statements. *See, e.g.*, PX 28 (Vera Dec.) Att. F, pp. 324-25.
[112] PX 29 (Aiken Dec.) Att. BB, p. 579. Because this figure included downloads of both the free and paid versions of the software, we cannot calculate total sales at this time, but we expect that figure to be substantial.

III. ARGUMENT

The Plaintiffs seek an *ex parte* TRO halting Defendants' ongoing violations of the FTC Act, the TSR, and the FDUTPA. The Plaintiffs request that the Court enjoin Defendants from these ongoing violations, freeze Defendants' assets to preserve them for restitution to victims, appoint a Temporary Receiver over the ICE Corporate Defendants, allow the Plaintiffs immediate access to the ICE Corporate Defendants' business premises and expedited access to the PC Cleaner Defendants' records, and permit limited expedited discovery. As set forth below, and supported by the Plaintiffs' exhibits, the evidence overwhelmingly supports entry of the proposed TRO.

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

Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), authorizes the Plaintiffs to seek, and this Court to grant, preliminary and permanent injunctive relief enjoining violations of Section 5 of the FTC Act and "any ancillary relief necessary to accomplish complete justice." *FTC v. USA Fin., LLC*, 415 Fed. Appx. 970, 976 (11th Cir. 2011); *AT&T Broadband v. Tech Commc'ns, Inc.*, 381 F.3d 1309, 1316 (11th Cir. 2004); *FTC v. IAB Mktg. Assocs., LP*, 972 F. Supp. 2d 1307, 1313 (S.D. Fla. 2013). The Court may also enter a temporary restraining order or other preliminary relief to preserve the possibility of providing effective final relief. *FTC v. Gem Merch. Corp.*, 87 F.3d 466, 468-69 (11th Cir. 1996); *FTC v. U.S. Oil & Gas Corp.*, 748 F.2d 1431, 1434 (11th Cir. 1984). Such ancillary relief is broad and may include an asset freeze to preserve assets for restitution to victims, the appointment of a receiver, immediate access to business premises, and expedited discovery – all forms of relief that courts in this District have granted in other cases recently filed by the FTC.[113]

[113] *See, e.g.*, *FTC v. Centro Natural Corp., et al.*, No. 14-CV-23879-CMA (S.D. Fla. Oct. 21, 2014) (entering *ex parte* TRO granting asset feeze, immediate access, expedited discovery and appointing receiver); *FTC v. Prime*

B. The Evidence Justifies Entry of a Temporary Restraining Order and a Preliminary Injunction

In considering a TRO or preliminary injunction under Section 13(b), this Court must: (1) determine the likelihood that the Plaintiffs will ultimately succeed on the merits; and (2) balance the equities. *FTC v. IAB Mktg. Assocs., LP*, 746 F.3d 1228, 1232 (11th Cir. 2014); *FTC v. Univ. Health, Inc.*, 938 F.2d 1206, 1217 (11th Cir. 1991). The Plaintiffs, unlike private litigants, need not prove irreparable injury, which is presumed. *Univ. Health*, 938 F. 2d at 1218. In balancing the equities, "the public interest should receive greater weight" than any private interest. *FTC v. World Wide Factors, Ltd.*, 882 F.2d 344, 347 (9th Cir. 1989); *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1029 (7th Cir. 1988); *FTC v. USA Beverages, Inc.*, No. 05-CV-61682, 2005 WL 5654219, at *8 (S.D. Fla. Dec. 6, 2005). *See also FTC v. Mallett*, 818 F. Supp. 2d 142, 149 (D.D.C. 2011) ("The public interest in ensuring the enforcement of federal consumer protection law is strong."). As demonstrated below, the evidence in this case satisfies this two-part test and warrants the issuance of a temporary restraining order against the Defendants.

1. The Plaintiffs Have Demonstrated a Likelihood of Success on the Merits

Plaintiffs must show that they will likely prevail on the merits, but need not present evidence to justify a "final determination" that Defendants violated the law. *Univ. Health*, 938 F.2d at 1218. As set forth below, Plaintiffs meet this requirement by showing that Defendants

---

Legal Plans LLC, et al., No. 12-CV-61872-RNS (S.D. Fla. Sept. 24, 2012) (same); *FTC v. IAB Mktg. Assocs., LP, et al.*, No 12-CV-61830-RNS (S.D. Fla. Sept. 18, 2012) (same); *FTC v. Premier Precious Metals, Inc., et al.*, No. 12-CV-60504-RNS (S.D. Fla. Mar. 20, 2012) (entering *ex parte* TRO granting asset freeze and immediate access and appointing receiver); *FTC v. VGC Corp. of Am., et al.*, No. 11-CV-21757-JEM (S.D. Fla. May 17, 2011) (entering *ex parte* TRO granting asset freeze, immediate access, and expedited discovery, and appointing receiver); *FTC v. Am. Precious Metals, LLC*, No. 11-CV-61072-RNS (S. D. Fla. May 10, 2011) (entering *ex parte* TRO granting asset freeze and immediate access and appointing receiver); *FTC v. U.S. Mortg. Funding, Inc., et al.*, No. 11-CV-80155-JIC (S.D. Fla. Feb. 20, 2011) (entering *ex parte* TRO granting asset freeze, immediate access, and expedited discovery and appointing receiver); *FTC v. Timeshare Mega Media & Mktg. Group, Inc., et al.*, 10-CV-62000-WJZ (S.D. Fla. Oct. 20, 2010) (same); *FTC v. 1st Guar. Mortgage Corp., et al.*, No. 09-CV-61840-JJO (S.D. Fla. Nov. 25, 2009) (same); *FTC v. First Universal Lending, LLC, et al.*, No. 09-CV-82322-WJZ (S.D. Fla. Nov. 19, 2009) (same); *FTC v. Kirkland Young, LLC, et al.*, No. 09-CV-23507-ASG (S.D. Fla. Nov. 19, 2009) (entering *ex parte* TRO granting asset freeze and immediate access and appointing receiver).

have violated and continue to violate Section 5 of the FTC Act, the TSR, and the FDUTPA.

a.) The Plaintiffs have Demonstrated a Likelihood of Success on the Merits that Defendants Violated Section 5(a) of the FTC Act

The voluminous evidence attached to the Plaintiffs' Motion demonstrates that Defendants have violated Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), the TSR, and the FDUTPA, which 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. *FTC v. People Credit First, LLC*, 244 Fed. Appx. 942, 944 (11th Cir. 2011) (following *FTC v. Tashman*, 318 F.3d 1273, 1277 (11th Cir. 2003)).

A misrepresentation is material if it involves facts that a reasonable person would consider important in choosing a course of action. *See FTC v. Cyberspace.com, LLC*, 453 F.3d 1196, 1201 (9th Cir. 2006). "Express claims, or deliberately made implied claims, used to induce the purchase of a particular product or service are presumed to be material." *Transnet Wireless Corp.*, 506 F. Supp. 2d at 1266. Implied claims are also presumed material if there is evidence that the seller intended to make the claim, *see, e.g., Novartis Corp. v. FTC*, 223 F.3d 783, 786-87 (D.C. Cir. 2000); *Kraft, Inc. v. FTC*, 970 F.2d 311, 322 (7th Cir. 1992), or if the claims go to the heart of the solicitation or the central characteristics of the product or service offered. *See FTC v. Figgie Int'l, Inc.*, 994 F.2d 595, 604 (9th Cir. 1993) (there is no loophole for implied deceptive claims). Moreover, in determining whether a solicitation is likely to mislead consumers, courts consider the overall "net impression" it creates. *FTC v. RCA Credit Servs., LLC*, 727 F. Supp. 2d 1320, 1329 (M.D. Fla. 2010) (citing *FTC v. Stefanchik*, 559 F.3d 924, 928 (9th Cir. 2009)). "A solicitation may be likely to mislead by virtue of the net impression it creates even though the solicitation also contains truthful disclosures." *Id.* (quoting *Cyberspace.Com*, 453 F.3d at 1200).

Plaintiffs need not prove that the misrepresentations were done with an intent to defraud or deceive, or were made in bad faith. *FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1202 (10th Cir. 2005). Nor does Plaintiffs 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. *Transnet Wireless*, 506 F. Supp. 2d at 1266-67. *See also FTC v. Verity Int'l, Ltd.*, 443 F.3d 48, 63 (2d Cir. 2006); *Figgie Int'l*, 994 F.2d at 605 ("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 explained above in detail, both the PC Cleaner Defendants and the ICE Defendants make misrepresentations to consumers. The PC Cleaner Defendants, through their software-based scans, convince consumers that they have identified problems on consumers' computers, including malware, system problems and privacy concerns.[114] These representations are false. The scan is designed to falsely identify problems on consumers' computers, exaggerate minor issues and otherwise deceive consumers into thinking that their computers are significantly compromised. For example, PC Cleaner Pro falsely identifies non-existent malware on a completely fresh installation of Windows and the free scan counts as "problems" many innocuous files such as temporary files, web browser cookies, and Windows default settings.[115]

The ICE Defendants, using their "diagnostic" sales pitch, convince consumers that they

[114] PX 2 (Beltran Dec.) ¶ 5; PX 6 (Daniel Dec.) ¶ 3; PX 13 (Prytko Dec.) ¶ 3.
[115] PX 30 (Kraemer Dec.) Att. A, p. 693; PX 18 (Skoudis Dec.) Att. A, pp. 72-73; PX 28 (Vera Dec.) Att. L, p. 362.

have identified problems on consumers' computers, including viruses, spyware, system errors and/or damage. In particular, using "msconfig" and the "Event Viewer" screen as demonstrable aids, the ICE Defendants tell consumers that their computers are likely to crash due to "running services" and "trace elements" that build up over time causing errors and computer crashes.[116] As discussed in Section II.B.1 & 2 above, these representations are false. In fact, the tools selected by the ICE Defendants and the manner in which they were used, makes it very unlikely that the ICE/ATS telemarketers could diagnose any actual security or performance issues on most consumers' computers.[117]

Moreover, these representations are likely to mislead consumers acting reasonably under the circumstances. Both the PC Cleaner Defendants and the ICE Defendants go to great lengths to trick consumers into believing that their computers are in immediate need of repair. The PC Cleaner Defendants use a convincing "system scan" that displays thousands of non-existent problems to induce consumers into purchasing PC Cleaner Pro.[118] The ICE Defendants not only state affirmatively that consumers' computers are damaged, but they also show consumers the errors and warnings in the Event Viewer, and misrepresent that the innocuous messages are actually cause for alarm.[119] Given this level of trickery and the number of consumers who have purchased their products, the Defendants' claims are likely to mislead reasonable consumers.

Finally, the Defendants' representations are material. Indeed, both the PC Cleaner Defendants and the ICE Defendants' false representations have induced consumers to pay

---

[116] PX 4 (Carr Dec.) ¶ 3; PX 9 (Green Dec.) ¶ 2; PX 10 (Harris Dec.) ¶ 4; PX 12 (Holmes Dec.) ¶ 7; PX 29 (Kraemer Dec.) ¶¶ 16-17; PX 14 (Reddin Dec.) ¶ 6; PX 15 (Rhodes Dec.) ¶ 6; PX 18 (Skoudis Dec.) Att. A, pp. 75-77; PX 28 (Vera Dec.) ¶ 16 & Att. A, p. 196.
[117] PX 18 (Skoudis Dec.), Att. A, p. 62.
[118] PX 2 (Beltran Dec.) ¶ 5; PX 6 (Daniel Dec.) ¶ 3; PX 30 (Kraemer Dec.) Att. A, p. 693; PX 13 (Prytko Dec.) ¶ 3; PX 18 (Skoudis Dec.) Att. A, p. 72; PX 28 (Vera Dec.) Att. L, p. 362.
[119] PX 4 (Carr Dec.) ¶ 3; PX 9 (Green Dec.) ¶ 2; PX 10 (Harris Dec.) ¶ 4; PX 11 (Heupel Dec.) ¶ 3; PX 12 (Holmes Dec.) ¶ 7; PX 30 (Kraemer Dec.) ¶ 17; PX 13 (Prytko Dec.) ¶ 4; PX 14 (Reddin Dec.) ¶ 6; PX 15 (Rhodes Dec.) ¶ 6; PX 28 (Vera Dec.) ¶ 17 & Att. A, pp. 197-99.

upwards of $750 for unnecessary computer repair services and computer security products they would not have otherwise purchased. It is difficult to imagine any consumer who would purchase the Defendants' products had the Defendants been candid about the fact that their telemarketers had no idea whether there was anything wrong with consumers' computers. Moreover, Defendants' claims are presumed to be material because they are express claims. *FTC v. Bronson Partners, LLC*, 564 F. Supp. 2d 119, 135 (D. Conn. 2008). *See also In re Thompson Medical Co.*, 104 F.T.C. 648, 818-19 (1984) *aff'd* 791 F.2d 189 (D.C. Cir. 1986).

b) The Plaintiffs Have Demonstrated a Likelihood of Success on the Merits that the ICE Defendants Violated the Telemarketing Sales Rule

In 1994, Congress directed the FTC to prescribe rules prohibiting abusive and deceptive telemarketing acts or practices pursuant to the Telemarketing Act. 15 U.S.C. §§ 6101-6108. The FTC then adopted the Telemarketing Sales Rule ("TSR"). 16 C.F.R. § 310. The ICE Defendants have repeatedly violated the TSR by making false or misleading statements to induce consumers to purchase their computer security or technical support services.

The TSR prohibits any seller or telemarketer from making a false or misleading statement to induce any person to pay for goods or services or to induce a charitable contribution. 16 C.F.R. § 310.3(a)(4). The ICE 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(aa), (cc), and (dd). Moreover, the TSR's prohibition against making false or misleading statements applies to all statements regarding upsells,[120] whether the statements were made during an outbound call initiated by the telemarketer or, as here, an inbound call initiated by a consumer. 16 C.F.R. § 310.6(4). As explained above, the ICE Defendants have falsely stated

[120] Consumers typically call the ICE/ATS telemarketers to activate software or obtain customer service assistance for another software program. PX 29 (Aiken Dec.) ¶ 76; PX 30 (Kraemer Dec.) ¶ 14; PX 28 (Vera Dec.) ¶¶ 13, 24. ICE/ATS uses these inbound calls to upsell additional products and services. PX 29 (Aiken Dec.) ¶ 76.

that they have identified problems on consumers' computers. The ICE Defendants made these statements to induce consumers to purchase computer security or technical support services, and in fact consumers have purchased these services. Therefore, the ICE Defendants have violated the TSR.

c) The State of Florida has Demonstrated a Likelihood of Success on the Merits that Defendants Have Violated the FDUTPA

The same representations that violate Section 5 of the FTC Act and the TSR also violate the FDUTPA. Section 501.204 of FDUTPA, Chapter 501, Part II, Florida Statutes, prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." Chapter 501, Part II, Florida Statutes (2012). In construing this Section, the Florida Legislature has declared that "due consideration and great weight shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a)(1) of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) as of July 1, 2006." *Id.* As explained in detail above, both the PC Cleaner Defendants and the ICE Defendants make misrepresentations to consumers. These misrepresentations are likely to mislead consumers acting reasonably under the circumstances and have induced consumers to pay hundreds of dollars for unnecessary computer products and services.

2. The Balance of Equities Mandates Preliminary Injunctive Relief

Given that the Plaintiffs have a strong likelihood of success on the merits, injunctive relief is warranted if the Court, weighing the equities, finds that relief is in the public interest. Here, the balance of equities mandates entry of a TRO because the public interest in preventing additional consumers from falling victim to Defendants' deceptive practices far outweighs any possible interest Defendants may have in continuing to operate their business deceptively. "[W]hen a district court balances the hardships of the public interest against a private interest,

the public interest should receive greater weight." *World Wide Factors*, 882 F.2d at 347; *World Travel Vacation Brokers, Inc.*, 861 F.2d at 1029. The public has a compelling interest in halting the Defendants' unlawful and injurious conduct and preserving assets that may be used for restitution to their victims. This interest is particularly strong because the Defendants' conduct has caused consumer loss exceeding a hundred million dollars. It is not an unreasonable burden to require the Defendants to cease their illegal conduct and comply with the law. The Defendants "can have no vested interest in a business activity found to be illegal." *United States v. Diapulse Corp. of Am.*, 457 F.2d 25, 29 (2d Cir. 1972) (internal quotations and citations omitted). In addition, it is likely that only the entry of the requested temporary and preliminary injunctive relief will prevent the Defendants from continuing to deceive and harm the public during the pendency of this litigation. Therefore, because the voluminous evidence attached to the Plaintiffs' Motion demonstrates that the Plaintiffs are likely to succeed on the merits, and the equities tip decidedly in the public's favor, a TRO is warranted.

3. The Corporate Defendants Operate as a Common Enterprise and are Jointly and Severally Liable for Each Other's Violations

The ICE Corporate Defendants and the PC Cleaner Corporate Defendants operate as common enterprises. To determine if a common enterprise exists, courts consider various factors, including whether the corporations: (1) maintain officers and employees in common; (2) operate under common control; (3) share office space; (4) operate the business through a maze of interrelated companies; (5) comingle funds; and (6) share advertising and marketing. *FTC v. Wash. Data Res.*, 856 F. Supp. 2d 1247, 1271 (M.D. Fla. 2012) (citations omitted).[121]

[121] *See, e.g.*, *FTC v. John Beck Amazing Profits, LLC*, 2012 U.S. Dist. LEXIS 70068, at *71-72 (C.D. Cal. April 20, 2012) (finding that corporate defendants who were controlled by the same individuals and shared the same business address and office space operated as a common enterprise); *FTC v. Grant Connect, LLC*, 827 F. Supp. 2d 1199,

The ICE Corporate Defendants conduct the business practices described above through an interrelated network of companies that have common ownership, officers, managers, employees, business functions, and office locations. For example, Deignan, Herdsman and Wright are all officers and managers of ICE, PC Vitalware, and Super PC Support.[122] The remaining ICE Corporate Defendant, ATS, operates solely as a d/b/a of ICE, and is managed by Deignan.[123] In addition, all of the ICE Corporate Defendants share the same two addresses (700 Banyan Trail and 4800 T Rex Avenue in Boca Raton) and use them interchangeably on corporate records, bank records, and in business correspondence.[124]

Furthermore, the ICE Corporate Defendants are interrelated. For example, (1) the ICE Defendants have registered "Advanced Tech Support" as fictitious name for ICE;[125] (2) in correspondence between Deignan and the BBB regarding the BBB's decision to revoke ICE/ATS's BBB accreditation, Deignan references his companies as "Inbound Call Experts d/b/a Advanced Tech Support;"[126] (3) ICE filed a complaint in Florida Circuit Court identifying itself as "Inbound Call Experts d/b/a Advanced Tech Support;"[127] (4) ICE is the registrant for the ICE

1216 (D. Nev. 2011) (finding that corporate defendants who were controlled by the same individuals, used the same employees, and operated out of the same office space operated as a common enterprise); *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1116 (S.D. Cal. 2008) (finding that corporate defendants who shared office space, employees, payroll funds and other expenses, and engaged in unified advertising operated as a common enterprise); *FTC v. LoanPointe*, 2011 U.S. Dist. LEXIS 104982 at *25 (D. Utah Sept. 15, 2011) (finding that the corporate defendants who had shared ownership and control, office space and addresses, and employees operated as a common enterprise); *FTC v. Think Achievement Corp.*, 144 F. Supp. 2d 993, 1012-13 (N.D. In. 2000) (finding that corporate defendants who were controlled by the same individual, shared office space and offices, had a network of interrelated companies, and moved funds among the companies operated as a common enterprise).

[122] PX 29 (Aiken Dec.) ¶¶ 27-29.

[123] *Id.* at ¶¶ 19-20.

[124] *Id.* at ¶¶ 19-22 & Att. GG, p. 631; PX 30 (Kraemer Dec.) ¶ 49.

[125] PX 29 (Aiken Dec.) ¶ 20 & Att. GG, p. 631.

[126] *Id.* at Att. GG, p. 624.

[127] *Id.* at ¶ 60.

Corporate Defendants' primary domain, advancedtechsupport.com;[128] and (5) ICE instructs its employees to tell consumers that they work for Advanced Tech Support.[129]

In addition, PC Vitalware and Super PC Support are also interrelated with the other ICE Corporate Defendants. Deignan and Herdsman are signatories on corporate bank accounts for PC Vitalware, Super PC Support and ICE.[130] PC Vitalware produces PCMRI software, one of the products that the ICE Corporate Defendants upsell to consumers.[131] Super PC Support advertises remote technical assistance on its websites and directs consumers to the ICE/ATS call center.[132] Accordingly, these entities operate as a common enterprise, and each entity is jointly and severally liable for the acts and practices of ICE, ATS, PC Vitalware or Super PC Support.

Similarly, the PC Cleaner Corporate Defendants also operate as a common enterprise. Each of the PC Cleaner Corporate Defendants is owned and operated solely by Myricks, most likely out of his home. He is the President of Netcom3 Global and PC Cleaner, and the CEO of Netcom3.[133] He also registered the domain pc-cleaners.com, a website that refers to the corporate entities together as "PC Cleaner Inc./Netcom3 Global, Inc."[134] Myricks also registered the domain netcom3global.com.[135] This website links to pc-cleaners.com, and the domain information for netcom3.com, although it is privacy protected, lists netcom3global.com as the website title.[136] Finally, PC Cleaner Pro, a product offered by PC Cleaner, is also available for download on the netcom3.com website.[137] Accordingly, these entities operate as a common

---

[128] PX 30 (Kraemer Dec.) Att. R, p. 935.
[129] PX 16 (Tomich Dec.) ¶ 5.
[130] PX 29 (Aiken Dec.) ¶ 57.
[131] PX 30 (Kraemer Dec.) ¶ 36; PX 1 (Barnes Dec.) ¶ 6; PX 6 (Ernst Dec.) ¶ 5.
[132] PX 30 (Kraemer Dec.) ¶¶ 30-31.
[133] PX 29 (Aiken Dec.) ¶ 30.
[134] PX 30 (Kraemer Dec.) ¶ 45 & Att. J, p. 843.
[135] *Id.* at ¶ 48.
[136] *Id.* at ¶¶ 48 & 52.
[137] PX 30 (Kraemer Dec.) Att. J, p. 842.

enterprise and each member of the enterprise is jointly and severally liable for the acts and practices of PC Cleaner, Netcom3 Global, or Netcom3.

4. The Individual Defendants are Liable

The Individual Defendants are liable for their own violations of the FTC Act, the TSR, and the FDUTPA, as well as the Corporate Defendants' illegal practices. Once the Plaintiffs establish that a corporate defendant violated Section 5 of the FTC Act, individual defendants will be personally liable for injunctive and monetary relief if the individual defendant: (1) participated directly in the deceptive acts or practices or had the authority to control them; and (2) had some knowledge of the corporation's unlawful acts or practices. *Gem Merch. Corp.*, 87 F.3d at 470 (citing *FTC v. Amy Travel Serv., Inc.*, 875 F.2d 564, 573 (7th Cir. 1989)); *USA Fin., LLC*, 415 Fed. Appx. at 974-75.

With respect to the "participation or control" component: "[a]uthority to control a company's practices may be demonstrated by active participation in the corporate affairs, including assuming duties as a corporate officer." *RCA Credit Services, LLC*, No. 8:08-CV-2062-T-27AEP, 2010 WL 2990068, at *4; *Transnet Wireless Corp.*, 506 F. Supp. 2d at 1270. Bank signatory authority or acquiring services on behalf of a corporation is also evidence of authority to control. *FTC v. USA Fin. LLC.*, 415 Fed. Appx. at 974-75.

The role of each Individual Defendant is discussed in Section II.C. The Individual Defendants have all served as officers and owners of one or more of the entities comprising the respective common enterprises. As such, each had authority to control the misconduct at issue. Further, each of these individuals has played an active role in the management and/or operation of one or more Corporate Defendants. Among other things, the Individual Defendants have

acted as signatories on corporate accounts,[138] paid for operating and business expenses,[139] responded to consumer complaints,[140] or registered the Corporate Defendants' domains.[141]

Plaintiffs can prove the requisite level of knowledge by showing that the individual: (1) had actual knowledge of material misrepresentations; (2) was recklessly indifferent to the truth or falsity of such misrepresentations; or (3) had an awareness of a high probability of fraud along with intentional avoidance of the truth. *FTC v. FTN Promotions, Inc.*, No. 8:07-CV-1279-T-30TGW, 2008 WL 821937, at *2 (M.D. Fla. March 26, 2008) (quotations and citation omitted). *See also FTC v. Crescent Publ'g Group, Inc.*, 129 F. Supp. 2d 311, 324 (S.D.N.Y. 2001); *FTC v. Five-Star Auto Club, Inc.*, 97 F. Supp. 2d 502, 535 (S.D.N.Y 2000); *FTC v. Minuteman Press*, 53 F. Supp. 2d 248, 259-60 (E.D.N.Y. 1998); *FTC v. Kitco of Nevada, Inc.*, 612 F. Supp. 1282, 1292 (D. Minn. 1985). The knowledge element does not require Plaintiffs to prove the individual defendant's subjective intent to defraud consumers. *USA Fin. LLC.*, 415 Fed. Appx. at 974 (*citing Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1368 (11th Cir. 1988)). Moreover, a defendant's degree of participation in the business is probative of knowledge. *FTC v. RCA Credit Servs.*, 727 F. Supp. 2d 1320, 1340 (M.D. Fla. 2010).

The evidence presented by the Plaintiffs demonstrates that the Individual Defendants have knowledge of the Corporate Defendants' illegal practices. Each of the Individual Defendants was aware of consumer complaints against the corporate entities. For example, Deignan's correspondence with the BBB confirms his knowledge of consumer complaints against his company.[142] Similarly, Wright exchanged e-mails with a malware researcher at ThreatTrack Security that demonstrate Wright's knowledge of both consumer complaints and the

[138] PX 29 (Aiken Dec.) ¶ 57.
[139] *Id.* at ¶¶ 41-42.
[140] *Id.* at ¶¶ 27, 30; PX 17 (Howes Dec.) Att. A, pp. 55-57.
[141] PX 29 (Aiken) ¶ 46; PX 30 (Kraemer Dec.) ¶¶ 45-53.
[142] PX 29 (Aiken Dec.) ¶ 27.

deceptive tactics his company was using.[143] Myricks recently settled a large class action in the United States District Court for the Central District of California concerning the very deceptive acts alleged in the Complaint.[144] Further, the BBB forwarded consumer complaints to Myricks. Although many of the consumers' complaints went unanswered, when the company did respond, Myricks provided the response.[145] Finally, Herdsman has actively participated in ICE's corporate affairs by being a corporate officer, a signatory on corporate bank accounts, the LogMeIn account holder, and the credit card holder who paid for numerous business expenses.[146] In light of his extensive involvement in the business operations, he either knew about consumer dissatisfaction or intentionally avoided the truth. Thus, the Individual Defendants have the requisite knowledge of the unlawful conduct.

C. An *Ex Parte* TRO With Additional Equitable Relief Is Necessary To Stop Defendants' Unlawful Conduct and Preserve Effective Financial Relief

As the evidence has shown, Plaintiffs will ultimately succeed in proving that the Defendants are engaging in deceptive practices in violation of the FTC Act and the FDUTPA, and are violating the TSR, and that the balance of equities strongly favors the public interest. Preliminary injunctive relief is thus warranted. Federal Rule of Civil Procedure 65(b) permits this Court to grant a temporary restraining order on an *ex parte* basis if there is a clear showing that "immediate and irreparable injury, loss, or damage will result" if notice is given. FED. R. CIV. P. 65(b). *See also In re Vuitton et Fils*, 606 F.2d 1, 4-5 (2d Cir. 1979).

For several years, the ICE Defendants have been engaged in a deceptive tech support scheme that has harmed hundreds of thousands of consumers and caused consumer injury exceeding a hundred million dollars. In addition, the PC Cleaner Defendants have continued

[143] *See supra* Section II.C.4.
[144] PX 29 (Aiken Dec.) ¶ 30.
[145] *Id.*
[146] PX 29 (Aiken Dec.) ¶¶28 & 41-42.

to deceptively market security software despite settling a class action lawsuit filed against them. This conduct alone supports the inference that the Defendants will continue their illegal conduct absent a court order. *See SEC v. Management Dynamics, Inc.*, 515 F. 2d 801, 807 (2d Cir. 1975) ("the commission of past illegal conduct is highly suggestive of the likelihood of future violations").

In order to stop Defendants' unlawful activities and to preserve the Court's ability to grant the final relief sought, the Court should enter an *ex parte* TRO that: (1) prohibits Defendants from engaging in conduct that violates the FTC Act, the TSR and the FDUTPA; (2) freezes Defendants' assets; (3) appoints a temporary receiver over the ICE Corporate Defendants; (4) grants the Plaintiffs and the temporary receiver immediate access to the ICE Defendants' business premises; and (5) authorizes limited expedited discovery.

1. The Court Should Stop the Defendants' Ongoing Scam

To prevent ongoing consumer injury, the Court should enter a TRO that immediately prohibits Defendants from engaging in any conduct that violates the FTC Act, the TSR or the FDUTPA, including making misrepresentations concerning the identification of computer problems on consumers' computers. The Court should also enter a TRO that includes provisions directing telephone carriers and webhosting companies to disable the Defendants' telephone numbers and websites to prevent further consumer injury. The Defendants rely on their phone numbers and websites to lure consumers into their schemes, disseminate their deceptive marketing, and process payments from consumers. Other courts have granted similar relief against defendants who have used Internet websites to promote fraud.[147]

[147] *See, e.g., FTC v. Pecon Software, et al.*, No. 12-cv-7186 (S.D.N.Y. Sept.25, 2012) (granting *ex parte* TRO that enjoined Defendants from violating the FTC Act and the TSR and disconnected Defendants' telephone numbers and suspended their websites); *FTC v. Navestad* No. 09-6329 (W.D.N.Y. June 25, 2009) (granting *ex parte* TRO that enjoined Defendants from violating the FTC Act and suspended Defendant's websites); *FTC v. Edge Solution, Inc.*

As discussed above, this Court has broad equitable authority under Section 13(b) of the FTC Act to grant ancillary relief necessary to accomplish complete justice. *Amy Travel*, 875 F.2d at 571-72; *FTC v. H.N. Singer, Inc.*, 668 F.2d 1107, 1113 (9th Cir. 1982). *See also FTC v. Five-Star Auto Club*, 97 F. Supp. 2d 502, 532-39 (S.D.N.Y. 2000). These requested prohibitions do no more than order that Defendants comply with the law. Moreover, because Defendants have continued their unlawful business practices unabated despite having notice from hundreds of consumer complaints, an anti-virus vendor blocking a corporate domain, and a class action lawsuit, immediate injunctive relief is necessary to protect additional consumers from being harmed by Defendants' ongoing unlawful practices.

2. The Court Should Freeze Defendants' Assets to Preserve the Possibility of Providing Restitution to Defendants' Victims

As part of the permanent relief in this case, the Plaintiffs seek monetary redress for consumers victimized by Defendants' unlawful practices. To preserve the availability of funds to provide such equitable relief, Plaintiffs request that the Court issue an order requiring the preservation of assets and evidence. The Eleventh Circuit has repeatedly upheld the authority of district courts to order an asset freeze to preserve the possibility of consumer redress (*see, e.g., Gem Merch. Corp.*, 87 F.3d at 469; *U.S. Oil & Gas Corp.*, 748 F.2d at 1433-34), and courts in this District have frozen defendants' assets in numerous FTC enforcement actions.[148] An asset freeze is appropriate once the Court determines that the FTC is likely to prevail on the merits and restitution would be an appropriate final remedy. *World Travel*, 861 F.2d at 1031.

No. 07-4087 (E.D.N.Y. Oct 12, 2007) (same); *FTC v. Career Hotline*, No. 09-1483 (M.D. FL. Sept. 8, 2009) (court ordered in its preliminary injunction the disconnection of the Defendants' phone numbers).

[148] *See, e.g., FTC v. FMC Counseling Servs., Inc.*, No. 0:14-cv-61545 (S.D. Fla. July 7, 2014); *FTC v. 7051620 Canada, Inc.*, No. 1:14-cv-22132 (S.D. Fla. June 12, 2014); *FTC v. Your Yellow Pages, Inc.*, No. 1:14-cv-22129 (S.D. Fla. June 12, 2014); *FTC v. Southeast Trust, LLC*, No. 12-cv-62441 (S.D. Fla. Dec. 11, 2012); *FTC v. Shopper Systems, LLC*, No. 0:12-cv-23919 (S.D. Fla. Oct. 31, 2012); *FTC v. Prime Legal Plans LLC*, No. 0:12-cv-61872 (S.D. Fla. Sept. 24, 2012); *FTC v. IAB Marketing Associates, LP*, No. 0:12-cv-61830 (S.D. Fla. Sept. 18, 2012); *FTC v. Premier Precious Metals, Inc.*, No. 0:12-cv-60504 (S.D. Fla. Mar. 20, 2012); *FTC v. U.S. Mortgage Funding, Inc.*, No. 11-CV-80155 (S.D. Fla. Feb. 20, 2011).

"A party seeking an asset freeze must show a likelihood of dissipation of the claimed assets, or other inability to recover monetary damages, if relief is not granted." *Johnson v. Couturier*, 572 F.3d 1067, 1085 (9th Cir. 2009); *SEC v. First Fin. Group of Tex.*, 645 F.2d 429, 438 (5th Cir. 1981). In *Johnson*, the Ninth Circuit upheld an asset freeze because plaintiffs had established they were "likely to succeed in proving that [the defendant] impermissibly awarded himself tens of millions of dollars." 572 F.3d at 1085. Courts have also concluded that an asset freeze is justified where a defendant's business is permeated with fraud. *See, e.g., SEC v. Manor Nursing Ctrs., Inc.*, 458 F.2d 1082, 1106 (2d Cir. 1972); *First Fin. Group*, 645 F.2d at 438. Further, the Court can order an asset freeze whether the assets are inside or outside the United States. *United States v. First Nat'l City Bank*, 379 U.S. 378, 384 (1965).

An asset freeze is necessary here to preserve the status quo, ensure that funds do not disappear during the course of this action, and preserve the remaining assets for consumer redress and disgorgement. The PC Cleaner Defendants have demonstrated through past actions that they have no intention of complying with the law. Myricks was sued by the FTC for a deceptive Internet download scheme in 2005.[149] Rather than finding legitimate work, Myricks turned to another deceptive scheme and was recently sued by private plaintiffs in California in a class action lawsuit for the same conduct at issue here.[150] Despite a settlement order that requires him to change his marketing for PC Cleaner Pro, he has not made a single change.[151] An asset freeze as to the PC Cleaner Defendants is necessary because the business is permeated by fraud.

Similarly, an asset freeze is required for the ICE Defendants as well. In addition to taking millions of dollars from consumers through their deceptive scheme, the ICE Defendants

[149] PX 29 (Aiken Dec.) ¶ 62.
[150] *Id.* at ¶ 61.
[151] PX 30 (Kraemer Dec.) ¶ 42.

have, in the past two years, transferred collectively $10.1 million to three corporate entities owned and controlled by the ICE Individual Defendants, but with no obvious corporate presence or purpose.[152] In addition, the ICE Defendants have transferred approximately $11.3 million to an offshore bank account in Canada in the name of ICE Venture Capital Corporation.[153] These transfers indicate a serious risk that the Defendants' funds may disappear quickly and that corporate assets in the US might already be insufficient to provide consumer victims with full redress. As such, an asset freeze is critical to preserve whatever funds remain so that they can be used to pay redress to consumers injured by Defendants' unlawful conduct, and the balance of equities favors such relief. Moreover, the freeze here should extend to individual assets as well as corporate assets, because – as demonstrated above – the Plaintiffs are likely to succeed in showing that the individual defendants are liable for restitution. *World Travel*, 861 F.2d at 1031.

Moreover, the court in *FTC v. Equifin International. Inc.*, stated that "the nature of [an Internet marketing] business is such that Defendants *and their assets* could easily vanish at a moment's notice, and Defendants could just as easily set up operations at another location under a different name (all that is needed is a room, [computer] and postal drop)." 1997 U.S. Dist. LEXIS 10288, *33, *43 (C.D. Cal. 1997) (emphasis added) (granting preliminary injunction with asset freeze against fraudulent telemarketers). The FTC's experience in prior cases confirms this, as numerous defendants in other cases who were engaging in similarly serious unlawful practices have dissipated assets upon learning of an impending law enforcement action.[154] Under these circumstances, the risk of dissipation is high, and a temporary asset freeze is therefore necessary to preserve the Court's ability to award consumer redress.

---

[152] PX 27 (George Dec.) ¶¶ 11-13; PX 29 (Aiken Dec.) ¶¶ 27-29.
[153] PX 27 (George Dec.) ¶¶ 20-21; PX 29 (Aiken Dec.) ¶¶ 58-59.
[154] *See* Rule 65(B)(1) Certification of Federal Trade Commission Counsel Colleen Robbins in Support of Ex Parte Motion For A Temporary Restraining Order and Motion To Temporarily Seal Docket and Entire File, filed herewith.

3. The Court Should Appoint a Temporary Receiver Over the ICE Corporate Defendants

The Court should also appoint a temporary receiver over the ICE Corporate Defendants pursuant to the Court's equitable powers under Section 13(b) of the FTC Act. *U.S. Oil & Gas*, 748 F.2d at 1432. Appointment of a temporary receiver is appropriate where, as here, there is "imminent danger of property being lost, injured, diminished in value or squandered, and where legal remedies are inadequate." *Leone Indus. v. Assoc. Packaging, Inc.*, 795 F. Supp. 117, 120 (D.N.J. 1992). When a corporate defendant has used deception to obtain money from consumers, "it is likely that, in the absence of the appointment of a receiver to maintain the status quo, the corporate assets will be subject to diversion and waste" to the detriment of victims. *First Fin. Group of Tex.*, 645 F.2d at 438; *SEC v. Keller Corp.*, 323 F.2d 397, 403 (7th Cir. 1963).

Appointment of a receiver is particularly appropriate here because the ICE Corporate Defendants' deceptive acts and practices demonstrate that the ICE Corporate Defendants are likely to frustrate the Plaintiffs' law enforcement efforts by destroying evidence and/or dissipating assets. The receiver will help prevent the ICE Corporate Defendants from disposing of ill-gotten funds by identifying, securing, and controlling the use of the ICE Corporate Defendants' assets, as well as marshaling and preserving their records. The receiver will also assist in determining the full extent of the fraud and identifying additional victims of the ICE Corporate Defendants' scheme. For these reasons, the Court should appoint a temporary receiver over the ICE Corporate Defendants.

4. The Court Should Grant Expedited Discovery, Turnover of Business Records, and Immediate Access to the ICE Corporate Defendants' Business Premises

In order to locate documents and assets related to the Defendants' scam, the TRO should authorize the Plaintiffs to engage in expedited discovery, order the turnover of the PC Cleaner Defendants' business records, and allow the Plaintiffs and the temporary receiver immediate access to the ICE Corporate Defendants' business premises and records.[155] This relief is critical to the Plaintiffs', the receiver's, and the Court's ability to understand fully: (a) the scope of Defendants' business operations, their financial status, the participants involved, and their roles in the scheme; (b) the full range and extent of the Defendants' law violations; (c) the identities of injured consumers; (d) the total amount of consumer injury; and (e) the nature, extent, and location of the Defendants' assets.

Moreover, this relief is also necessary to protect against evidence destruction. As explained more fully in the Rule 65(b) Declaration of Counsel Colleen B. Robbins ("Robbins Certification"), in the FTC's experience, it is likely that the Defendants will take steps to destroy documents that relate to their scams. The proposed order includes provisions designed to grant access to Defendants' documents before they can be destroyed.[156] Courts in this District have granted *ex parte* TROs that include these provisions.[157] Accordingly, the Court should enter a temporary restraining order granting the Plaintiffs and the receiver immediate access and authorizing a turnover of business records and limited expedited discovery.

---

[155] The Plaintiffs are seeking a turnover of business records provision for the PC Cleaner Defendants because Myricks does not appear to have a business premise, and likely operates his business out of his home.
[156] District courts have broad and flexible authority in equity to depart from routine discovery procedures and applicable time frames, particularly in cases involving the public interest. *See* Fed. R. Civ. P. 26(d), 33(a), 34(b); *Porter v. Warner Holding Co.*, 328 U.S. 395, 398 (1946).
[157] *See supra* note 113.

5. The Court Should Issue the TRO *Ex Parte*

The substantial risk of asset dissipation and document destruction in this case, coupled with Defendants' ongoing and deliberate statutory violations, justifies *ex parte* relief without notice. Federal Rule of Civil Procedure 65(b) permits this Court to enter *ex parte* orders upon a clear showing that "immediate and irreparable injury, loss, or damage will result" if notice is given. *Ex parte* orders are proper in cases where "notice to the defendant would render fruitless the further prosecution of the action." *Am. Can Co. v. Mansukhani*, 742 F.2d 314, 322 (7th Cir. 1984). *See also Granny Goose Foods, Inc. v. Bhd. of Teamsters*, 415 U.S. 423, 439 (1974); *In re Vuitton et Fils, S.A.*, 606 F.2d 1, 4-5 (2d Cir. 1979). In cases involving pervasive fraud, "it [is] proper to enter the TRO without notice, for giving notice itself may defeat the very purpose for the TRO." *Cenergy Corp. v. Bryson Oil & Gas P.L.C.*, 657 F. Supp. 867, 870 (D. Nev. 1987).[158] Mindful of this problem, Courts in this District have regularly granted the FTC's request for *ex parte* TROs in Section 13(b) consumer fraud cases to preserve the possibility of full and effective final relief.[159]

As discussed above in Section II, Defendants' business operations are permeated by, and reliant upon, deceptive practices, and experience has shown that defendants engaged in fraudulent schemes often dissipate assets and destroy records if they receive notice of an impending FTC enforcement action. *See* Robbins Certification filed herewith. Such a risk is particularly high in this case. As to the PC Cleaner Defendants, moving forward on an *ex parte* basis is further justified because Myricks is a recidivist who is already violating the terms of a

[158] Providing notice in this matter could also prejudice the related case, *FTC v. Vast Tech, et. al.* (filed concurrently to this case), by tipping off the Defendants in that case. Although ICE/ATS and Vast Tech are competitors, they share many former and current employees and a geographic proximity that makes it likely that Vast Tech would immediately learn of any noticed action by the Plaintiffs, leading to dissipation of assets and destruction of documents relevant to both litigations.

[159] *See supra* n.113.

prior FTC order with this conduct.[160] In addition, he has failed to implement changes to the PC Cleaner Pro software scan required by a recent class action settlement.[161] The ICE Defendants continue to operate in the same deceptive manner despite numerous complaints from the BBB, a revocation of their BBB accreditation due to excessive complaints, and a security company blocking their primary domain due to complaints.[162]

Moreover, both the PC Cleaner Defendants and the ICE Defendants have used numerous techniques to hide their identities from consumers. For example, the PC Cleaner Defendants list three different "corporate" addresses on their publicly-available websites and corporate documents but, in reality, those addresses are merely post office boxes.[163] The ICE Defendants pay software and security companies to direct consumers unknowingly to their call center.[164] As a result, consumers do not always know which company they have called.[165] Both sets of Defendants also have used privacy protection services to hide their domains' contact information.[166] This contact information is key for consumers and law enforcement to determine the person responsible for a particular domain.[167] In addition, both sets of Defendants use a payment processor, Safecart, that effectively shields their own identity from consumers because the contact information that appears on consumers' credit card statements is for Safecart.[168]

Finally, the ICE Defendants have withdrawn millions of dollars and deposited the money into a corporate account in Canada and other business accounts controlled by the Individual ICE

---

[160] PX 29 (Aiken Dec.) ¶ 30.
[161] PX 30 (Kraemer Dec.) ¶ 42.
[162] PX 29 (Aiken Dec.) ¶¶ 87-88; PX 17 (Howes Dec.) ¶ 3.
[163] PX 29 (Aiken Dec.) ¶¶ 109-11.
[164] *Id.* at 73-74.
[165] *See* PX 2 (Beltran) ¶¶ 4 & 9; PX 13 (Prytko) ¶¶ 3 & 6-7.
[166] PX 30 (Kraemer Dec.) ¶¶ 50 & 52.
[167] *Id.* at ¶ 44.
[168] PX 29 (Aiken Dec.) ¶¶ 100-03, 107-08; PX 28 (Vera Dec.) Att. F, pp. 324-25.

Defendants.[169] Under these circumstances, there is a strong likelihood that Defendants would conceal or dissipate assets absent *ex parte* relief. As such, it is in the interest of justice to provide the requested *ex parte* relief to prevent the dissipation of assets or the destruction of evidence, which in turn will maintain the status quo and preserve this Court's ability to award full and effective final relief.

IV. CONCLUSION

The Defendants do not operate a legitimate business. The Defendants team up to dupe consumers into believing that their computers are in immediate need of repair in order to sell them expensive and unnecessary computer repair services. In order to put an end to these unlawful practices, the Plaintiffs request that this Court grant the Plaintiffs' motion for an *ex parte* TRO and ancillary equitable relief.

Respectfully submitted,

JONATHAN NEUCHTERLEIN
General Counsel

Dated: November 10, 2014

Colleen B. Robbins, Special Bar # A5500793
Emily Cope Burton, Special Bar # A5502042
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2548; crobbins@ftc.gov
(202) 326-2728; eburton@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

[169] PX 29 (Aiken Dec.) ¶¶ 58-59; PX 27 (George Dec.) ¶¶ 11-13 & 20-21.

PAMELA JO BONDI
ATTORNEY GENERAL
STATE OF FLORIDA

Dated: November 10, 2014

Katherine A. Kiziah
Assistant Attorney General
Florida Bar Number 0017585
1515 N. Flagler Drive
Suite 900
West Palm Beach, Florida 33401
(561) 837-5007
Attorney for Plaintiff
STATE OF FLORIDA