UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

FEDERAL TRADE COMMISSION,

STATE OF CONNECTICUT,
OFFICE OF ATTORNEY GENERAL, and

COMMONWEALTH OF PENNSYLVANIA,
OFFICE OF ATTORNEY GENERAL,

Plaintiffs,

v.

CLICK4SUPPORT, LLC,
a Connecticut limited liability company,

ISOURCEUSA LLC,
also d/b/a Click4Support and UBERTECHSUPPORT,
a Pennsylvania limited liability company,

INNOVAZION INC.,
also d/b/a Click4Support Tech Services, a Connecticut corporation,

SPANNING SOURCE LLC,
also d/b/a Click4Support,
a Pennsylvania limited liability company,

BRUCE BARTOLOTTA,
also known as Bruce Bart, individually and as an owner and officer of Click4Support, LLC and Innovazion Inc.,

FILED UNDER SEAL

CASE NO. _____

MEMORANDUM IN SUPPORT OF PLAINTIFF FTC'S *EX PARTE* MOTION FOR A TEMPORARY RESTRAINING ORDER WITH ASSET FREEZE AND OTHER EQUITABLE RELIEF AND FOR AN ORDER TO SHOW CAUSE WHY A PRELIMINARY INJUNCTION SHOULD NOT ISSUE

GEORGE SAAB,
individually and as an owner and officer of iSourceUSA LLC and Spanning Source LLC,

CHETAN BHIKHUBHAI PATEL,
individually and as an owner and officer of iSourceUSA LLC and Spanning Source LLC, and

NIRAJ PATEL,
individually and as an owner of iSourceUSA LLC and Spanning Source LLC,

Defendants.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Regulations

I. INTRODUCTION

Plaintiff Federal Trade Commission ("FTC" or "Commission") respectfully requests that the Court halt a technical support scam that has bilked tens of thousands of consumers throughout the United States out of millions of dollars by creating and then exploiting consumers' fears about vulnerabilities in their computers.[1] Defendants trick consumers into calling their telemarketing boiler rooms using misleading internet search engine-based advertising ("internet ads") and popup warning messages ("popups"). Once they get consumers on the telephone, Defendants misrepresent their affiliation with well-known U.S. technology companies. Next, they convince consumers to allow them to remotely access consumers' computers. Once they have control over the computers, they scare consumers into believing that the computers are infected with viruses, spyware, or other malware, are being hacked, or are otherwise compromised. Then, they peddle their computer security or technical support services (collectively, "technical support services") and charge consumers hundreds or even thousands of dollars for these unnecessary services.

Because Defendants operate a pernicious scheme that has inflicted and continues to inflict significant harm on unsuspecting consumers, the FTC seeks a temporary restraining order that halts Defendants' unscrupulous business practices, freezes assets, and preserves evidence, among other things. Defendants' widespread and persistent pattern of lies and deception,

[1] The FTC submits 70 exhibits in support of its Motion, including sworn declarations from consumer victims, an FTC investigator who conducted and recorded undercover calls to Defendants while posing as a consumer, a computer and information security expert who analyzed the data generated from the undercover calls, and representatives of U.S. technology companies. The exhibits also include business documents obtained from third-party entities. Exhibits are marked with and cited as "PX [number]" and, where appropriate, followed by a unique document identifier and/or the page number(s). Declarations are cited as "PX [number], [name] Decl., ¶ [number], Attach. [letter]." Transcripts of the undercover calls conducted by the FTC are cited as "PX [number], [Call One Tr., Call Two Tr., or Call Three Tr.], pp:ln1-ln2," where "pp" is the page number, "ln1" is the first cited line, and "ln2" is the last cited line.

coupled with their efforts to hide themselves, demonstrate their willingness to violate the law and to disregard such a temporary restraining order. For this reason, the FTC seeks this preliminary relief *ex parte*. Granting the FTC's Motion would prevent further harm to consumers and would preserve the Court's ability to grant effective final relief.

II. THE PARTIES

A. Plaintiffs

The FTC is an independent agency of the United States Government created by the FTC Act, 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), and the Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310. Section 13(b) of the FTC Act authorizes the FTC to bring suit in district court to enjoin violations of the laws it enforces and to secure appropriate equitable relief. 15 U.S.C. § 53(b). Similarly, the State of Connecticut, Office of Attorney General, ("CT AG") and the Commonwealth of Pennsylvania, Office of Attorney General, ("PA AG") are authorized to enjoin law violations and to seek appropriate relief pursuant to the Connecticut Unfair Trade Practices Act ("CUTPA") and the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("Pa UTPCPL"), respectively.

B. Defendants

Defendant **Click4Support, LLC ("C4S-CT")** is a Connecticut limited liability company created on March 21, 2014, with its principal place of business at 12 Main Street, Suite 1, Essex, Connecticut and an additional business address at 12 Penns Trail, Suite 12200, Newtown, Pennsylvania.[2] C4S-CT is owned and operated by Defendant Bruce Bartolotta,[3] and it is also

[2] PX 24; *see also* PX 70, DeWaide Decl., Attachs. A, D (lists 12 Main Street address in the service agreement and the 12 Penns Trail address in the proof of voided transactions).

[3] PX 24.

operated by Defendant George Saab.[4] C4S-CT uses www.click4support.net,[5] www.ubertechsupport.com,[6] and www.tekdex.com[7] as its business websites. As detailed below, C4S-CT deceptively markets and sells technical support services to consumers throughout the United States.

Defendant **iSourceUSA LLC ("iSourceUSA")** is a Pennsylvania limited liability company formed on September 3, 2013, with its principal place of business at 12 Penns Trail, Suite 12200, Newtown, Pennsylvania, and it has also been doing business as "Click4Support" since at least October 27, 2014, and as "UBERTECHSUPPORT" (or "Uber Tech Support") since at least May 13, 2015.[8] iSourceUSA is owned and operated by individual Defendants George Saab, Chetan Bhikhubhai Patel, and Niraj Patel and by corporate Defendants Innovazion Inc. and Spanning Source LLC.[9] iSourceUSA uses or has used several other addresses in Pennsylvania and New Jersey, all of which Defendant Spanning Source LLC also uses or has used.[10] iSourceUSA uses www.click4support.com[11] and www.ubertechsupport.com[12] as its business websites. As detailed below, iSourceUSA deceptively markets and sells technical support services to consumers throughout the United States.

Defendant **Innovazion Inc. ("Innovazion")** is a Connecticut corporation organized on June 28, 2011, with its principal place of business at 12 Main Street, Suite 1, Essex, Connecticut,

[4] *See, infra*, Section III.C.2.

[5] PX 18 (copy of www.click4support.net captured on Apr. 20, 2015).

[6] PX 20 (copy of www.ubertechsupport.com captured on June 9, 2015). C4S-CT directs consumers to this website to complete purchase transactions. *See* PX 1, Vega Decl., ¶¶ 55, 66.

[7] Within www.click4support.net and www.ubertechsupport.com, consumers can click on "Log a Ticket," which directs consumers to www.tekdex.com. *See* PX 21 (copy of www.tekdex.com as captured on Apr. 21, 2015).

[8] PX 25.

[9] *Id.*

[10] *Id.*; *see also* PX 6, p. 6.

[11] PX 17 (copy of www.click4support.com captured on Apr. 20, 2015).

[12] PX 20. Like C4S-CT, iSourceUSA directs consumers to this website to complete purchase transactions. *See* PX 1, ¶¶ 87-88.

and it has also been doing business as "Click4Support Tech Services" since at least November 27, 2014.[13] Innovazion is owned and operated by Defendant Bruce Bartolotta, and it has an ownership interest in iSourceUSA.[14] Innovazion uses www.c4sts.com[15] and www.tekdex.com[16] as its business websites. As detailed below, Innovazion deceptively markets and sells technical support services to consumers throughout the United States.

Defendant **Spanning Source LLC ("Spanning Source")** is a Pennsylvania limited liability company formed on July 9, 2007, with its principal place of business at 853 Second Street Pike, Suite B107, Richboro, Pennsylvania, and it has also been doing business as "Click4Support" since at least August 3, 2012.[17] It is owned and operated by Defendants George Saab, Chetan Bhikhubhai Patel, and Niraj Patel, and it has an ownership interest in iSourceUSA.[18] Spanning Source uses or has used several other addresses in Pennsylvania, New Jersey, and Massachusetts, all but one of which are also used by iSourceUSA or one of the individual Defendants.[19] Spanning Source uses www.click4support.com,[20] www.click4support.net,[21] www.ubertechsupport.com,[22] and www.tekdex.com[23] as its business websites. As detailed below, Spanning Source deceptively markets and sells technical support services to consumers throughout the United States.

---

[13] PX 6, pp. 3-6; PX 26.
[14] PX 25; PX 26.
[15] PX 19 (copy of www.c4sts.com captured on Aug. 3, 2015).
[16] Within www.c4sts.com, consumers can click on "Log a Ticket," which directs consumers to www.tekdex.com.
[17] PX 6, pp. 35-36; PX 27.
[18] PX 25; PX 27.
[19] PX 6, pp. 12-14; PX 7, pp. 6, 13; PX 8; PX 27.
[20] PX 6, pp. 12-14.
[21] *Id.*, p. 40.
[22] *See*, *supra*, Footnotes 6, 12.
[23] *See*, *supra*, Footnote 7.

Defendant **Bruce Bartolotta, also known as "Bruce Bart,"[24] ("Bartolotta")** resides in Deep River, Connecticut.[25] He is an owner, officer, and registered agent of C4S-CT.[26] He is an owner, chief financial officer, secretary, director, and registered agent of Innovazion.[27] Through Innovazion, he has an ownership interested in iSourceUSA.[28]

Defendant **George Saab ("Saab")** resides in Stow, Massachusetts.[29] He is an owner and officer of iSourceUSA and Spanning Source[30] and is a business manager of C4S-CT.[31]

Defendant **Chetan Bhikhubhai Patel ("C. Patel")** resides in Newtown, Pennsylvania.[32] He is an owner and officer of iSourceUSA and Spanning Source.[33]

Defendant **Niraj Patel ("N. Patel")** resides in New Hope, Pennsylvania.[34] He is an owner and officer of iSourceUSA and Spanning Source.[35]

Defendants C4S-CT, iSourceUSA, Innovazion, and Spanning Source are referred collectively as "Corporate Defendants," and Defendants Bartolotta, Saab, C. Patel, and N. Patel are referred collectively as "Individual Defendants."

III. STATEMENT OF FACTS

Since at least 2013, Defendants have been perpetrating a "technical support scam" that uses deceptive scare tactics to induce consumers to purchase unnecessary services. Defendants have successfully bilked tens of thousands of consumers out of at least $17.9 million.[36]

---

[24] PX 6, pp. 3-6.
[25] PX 26.
[26] PX 2; PX 24; PX 67, Ando Decl., ¶ 8.
[27] PX 6, pp. 3-6; PX 26.
[28] PX 25; PX 26.
[29] PX 25.
[30] PX 25; PX 27.
[31] PX 14; PX 67, ¶ 10.
[32] PX 25.
[33] *Id.*; PX 27.
[34] PX 25.
[35] *Id.*; PX 27.

This Section details: (A) how the Defendants lure consumers into their scheme; (B) the Defendants' false representations; (C) the role each Individual Defendant has played in the scheme; (D) how the Corporate Defendants operate as a common enterprise; (E) the Defendants' attempts to conceal their identity; and (F) consumer injury.

A. Defendants Lure Consumers into Calling Their Telemarketers by Using Misleading Internet Advertisements and Popup Warning Messages.

Defendants lure consumers into calling their telemarketers using misleading internet advertisements. In numerous instances, consumers with technology issues used an internet search engine, such as Google, to do web searches related to their technology issues.[37] The search results included Defendants' internet ads, which listed Defendants' telephone number or a link to another website listing Defendants' telephone number. When consumers dialed the telephone number listed, they were connected to Defendants' telemarketers.[38] In a number of these instances, due to the Defendants' internet ads or the web searches consumers conducted, consumers believed that they were calling a legitimate U.S. technology company or its affiliate.[39]

In addition to internet ads, Defendants lure consumers into calling their telemarketers using misleading popup warning messages. In a number of instances, Defendants' popups

---

[36] *See, infra,* Section III.F.

[37] *See* PX 41, Birdwell Decl., Attach. A; PX 42, Brown Decl., ¶ 2; PX 44, Day Decl., ¶ 2; PX 46, Attachs. A-B; PX 48, Elkin Decl., ¶ 2; PX 49, Fagan Decl., ¶ 2 & Attach. A; PX 50, Fronckoski Decl., Attach. A; PX 51, Gall Decl., ¶ 2; PX 52, Attach. A; PX 54, Guardia Decl., ¶ 2; PX 55, Hennen-Bergman Decl., ¶ 2; PX 62, Puma Decl., ¶¶ 2-3; PX 63, Rychel Decl., Attach. A; PX 64, Zarka Decl., ¶¶ 2-3; PX 66, Sarkissian Decl., ¶ 2; PX 70, ¶ 2.

[38] *See* PX 41, Attach. A; PX 42, ¶ 2; PX 44, ¶¶ 2-3; PX 46, Dolan Decl., ¶ 2; PX 48, ¶ 5; PX 49, ¶ 2; PX 51, ¶ 2; PX 52, Gares Decl., ¶ 2; PX 59, Mendoza Decl., ¶ 2; PX 61, Pitkin Decl., ¶ 3; PX 62, ¶ 3; PX 63, Attach. A; PX 64, ¶ 2; PX 70, ¶ 2.

[39] *See, e.g.*, PX 62, ¶ 3 ("With the type of internet search that I ran, I believed that this company was a third party used by the manufacturer to repair my computer."); PX 40, Barry Decl., Attach. A (thought it was HP Support); PX 47, Duane Decl., Attach. A (same); PX 43, Chipman Decl., Attach. A (thought it was Apple); PX 44, ¶ 2 (thought it was Toshiba); PX 51, ¶ 2 (thought it was an "authorized tech firm with Google"); PX 55, ¶ 2 (thought it was Best Buy's Geek Squad); PX 63, Attach. A (thought it was Cox Customer Support); PX 70, ¶ 2 (thought it was Charter).

appeared while consumers visited third-party websites on the internet,[40] and some displayed the logo of a legitimate U.S. technology company.[41] The popups remained on consumers' computer screens, advised them about a purported problem with their computers—such as a virus, malware, or some other vulnerability—and instructed them to call the telephone number listed in order to resolve the problem.[42] When consumers dialed the telephone number listed, they were connected to Defendants' telemarketers.[43] In some instances, Defendants' popups made consumers believe that their computers were truly infected and that they were calling a legitimate U.S. technology company to address the problem.[44]

B. Defendants Make False Representations to Trick Consumers into Purchasing Their Technical Support Services.

1. Defendants' representations that they are part of or affiliated with well-known U.S. technology companies are false.

Once consumers are connected to Defendants, they explain their technology issues to Defendants' telemarketers, who assure them that Defendants can fix their issues.[45] In many instances, the telemarketers did not voluntarily disclose to consumers the real identity of their company, and when questioned by consumers, the telemarketers claimed that they are part of or affiliated with a well-known U.S. technology company, such as Microsoft, Google, Apple, or Dell.[46] Consumers believed Defendants' claim.[47]

---

[40] *See* PX 56, Johnson Decl., ¶ 2; PX 58, Kano Decl., ¶ 3; PX 60, Monroe-Santos Decl., ¶¶ 2-3, Attach. A; PX 65, Burgess Decl., Attach A.

[41] *See* PX 45, Dobberpuhl Decl., ¶ 2 (displayed Apple Safari logo); PX 58, ¶ 3 (same).

[42] *See* PX 45, ¶ 2; PX 56, ¶ 2; PX 58, ¶ 3; PX 65, Attach A.

[43] *See* PX 56, ¶ 4; PX 58, ¶¶ 3-4; PX 60, Attach. A.

[44] *See* PX 45, ¶ 4; PX 56, ¶ 3; PX 58, ¶ 3; PX 60, Attach. A.

[45] *See, e.g.*, PX 56, ¶ 4.

[46] *See, e.g.*, PX 40, Attach. A (claimed to be "technical support that deals with Microsoft"); PX 53, Graham Decl., Attach. A ("a Microsoft agent"); PX 60, Attach. A ("a senior certified Microsoft technician"); PX 63, Attach. A ("Microsoft technicians representing Cox"); PX 70, Attach. C (claimed to be from Charter and Microsoft); PX 51, ¶¶ 3-4 (claimed to be "Google Support" on two separate occasions); PX 57, Kale Decl., Attach. A. (claimed to be from

In fact, none of the Defendants is part of or affiliated with these well-known U.S. technology companies, and none is authorized to provide technical support services in the name of these legitimate companies.[48]

Indeed, Defendants' misrepresentations are designed simply to make consumers believe that they are dealing with a legitimate company and to trick consumers into allowing Defendants to remotely access their computers. In many instances, Defendants' trickery worked.[49] To gain remote access, Defendants directed consumers to www.c4s.us,[50] a website that Defendants own and operate, or to third-party websites, such as LogMeIn.com.[51] Then, Defendants instructed consumers to enter a code or download a software application to begin the remote access session.[52]

During three separate undercover calls to Defendants conducted by an FTC investigator on June 3, 2015 (individually, "Call One," "Call Two," and "Call Three"), Defendants directed the FTC investigator to the same LogMeIn.com remote-access website, provided him the

---

Apple on two separate occasions); PX 43, Attach. A (claimed to be from Apple); PX 46, Attach. A-B (same); PX 65, Attach A (same); PX 41, Attach. A (claimed to be "Apple iPhone Support"); PX 45, ¶ 10 ("licensed by and registered with Apple"); PX 49, Attach. A ("authorized tech support for Apple"); PX 44, Attach. A ("[W]e also handle Dell product.'"); PX 50, Attach. A ("[I] was told that yes they were affiliated with Dell."); *see also* PX 47, Attach. A (claimed to be "HP Support"); PX 48, ¶ 2 ("technical support for Comcast"); PX 54, Attach. A ("an employee of Brother International Printer Company"); PX 66, Decl., ¶ 3 ("work with AT&T"); PX 69, Brautigam Decl. ¶ 3 ("working with Best Buy").

[47] *See*, *supra*, Footnote 46.

[48] *See*, *e.g.*, PX 39, Yoakum Decl. (declaration by representative of Microsoft Corporation); PX 36, Vanderveer Decl. (Apple Inc.); PX 38, Stidvent Decl. (Dell Inc.); PX 37, De Palma Decl. (AT&T's Services, Inc.).

[49] *See* PX 40, ¶ 3 & Attach. A; PX 41, Attach. A; PX 42, ¶ 3; PX 43, Attach. A; PX 47, Attach. A; PX 48, ¶ 3; PX 49, Attach. A; PX 51, ¶ 4; PX 54, Attach. A.; PX 52, Attach. A; PX 53, Attach. A; PX 55, Attach. A; PX 56, ¶ 4; PX 58, ¶ 4; PX 59, Attach. A; PX 60, Attach. A; PX 61, ¶ 4; PX 62, ¶ 4; PX 64, Attach. A; PX 65, Attach A; PX 70, Attach. C.

[50] *See*, *e.g.*, PX 54, Attach. A.

[51] *See*, *supra*, Footnote 49.

[52] *Id.*

six-digit code to enter, and instructed him to click on the prompts to allow the remote access sessions.[53]

In all known instances, Defendants told consumers that they needed to access consumers' computers in order to fix consumers' technology issues[54]—even when the consumers' technology issues had nothing directly to do with their computers.[55] In fact, Defendants wanted to access the computers so they could scare consumers into believing that their computers were in imminent danger, as detailed below.

2. Defendants' representations that they have detected security or performance issues on consumers' computers, including viruses, spyware, malware, or the presence of hackers, are false.

During the remote access sessions, Defendants had complete control over consumers' computers and had the ability, for example, to view the computer screen, move the mouse or cursor, enter commands, run applications, and access stored information. At the same time, consumers saw what Defendants saw and did on their computers.[56]

Once Defendants controlled the computers, they performed various commands and actions purportedly to identify the cause of the consumers' technology issues. Then, they

[53] *See* PX 1, ¶¶ 47, 58, 85. The FTC conducted three separate undercover calls as part of its investigation of Defendants' business practices. The FTC investigator conducted the undercover calls on June 3, 2015, at approximately 9:12 A.M. ("Call One"), 11:00 A.M. ("Call Two"), and 1:45 P.M. ("Call Three"). During these undercover calls, the FTC investigator posed as a consumer and recorded his conversations with Defendants and the computer activity during the remote access sessions. *See generally* PX 1; PX 28, Davis Decl.; PX 29, Patel Decl.

[54] *See*, *supra*, Footnotes 49-50; *see also* PX 1, ¶¶ 47, 58, 85.

[55] *See*, *e.g.*, PX 41, Attach. A ("update" appeared on consumer's Apple iPhone); PX 57, ¶ 2 (lost Apple iPhone contacts); PX 47, Attach. A (printer issue); PX 52, Attach. A (same); PX 53, Attach. A (same); PX 54, ¶ 2 (same); PX 59, Attach. A (same); PX 49, ¶ 4 (issue with TV); PX 51, ¶ 2 (issue with email); PX 61, ¶¶ 2, 10 ("As it turned out, my email problem was only because I needed a new password."); PX 64, Attach. A ("[I] needed to have the password reset [on my router].").

[56] *See*, *e.g.*, PX 1, ¶¶ 47, 58, 85.

launched a slew of deceptive scare tactics designed to convince consumers that there are viruses, spyware, malware, or hackers in their computers.

a. Defendants use the computer's Event Viewer to scare consumers into believing that "Error" and "Warning" messages are evidence of computer viruses or other problems.

A common ploy that Defendants use is to show numerous "Error" and "Warning" messages in the computer's Event Viewer and claim that these messages are evidence of viruses or other critical problems in the computer.[57] For example, during Call Two, Defendants' telemarketer began to diagnose the FTC investigator's computer problem by prompting the Event Viewer.[58] He circled the "Error" and "Warning" messages and the number "107" on the Event Viewer.[59] Then, he said that "these are the number of critical errors and warnings" in the computer and that "these critical errors is [sic] for your IP and for your internet and for your devices."[60] Next, he showed the investigator that there was no "option to delete" the errors and warnings[61] but reassured the investigator, saying, "I will get it done for you."[62]

While the "Error" and "Warning" messages in the Event Viewer may appear alarming, their presence in a computer is not necessarily an indication of a security issue or a computer problem.[63] In fact, as computer forensic analyst Hal Pomeranz[64] explains, "[it] is normal for Windows systems to collect hundreds or thousands of such messages…. Reviewing the Event

[57] *See* PX 54, Attach. A; PX 62, ¶ 5; *see also* PX 1, ¶ 60.
[58] PX 1, ¶ 60; *see generally* PX 31, Call Two Tr., 13:17-15:18.
[59] *Id*. & Attach. E (screenshot of "Error" and "Warning" messages in Event Viewer).
[60] PX 1, ¶ 60.
[61] *Id*. & Attach. F (screenshot showing no option to delete the warning message).
[62] PX 1, ¶ 60.
[63] PX 35, Pomeranz Decl., Exh. A, ¶ 31.
[64] The FTC retained Mr. Pomeranz as an expert to analyze the data generated from all three undercover calls conducted on June 3, 2015. The data includes, among other things, the audio and video recordings of the undercover calls and forensic images of the FTC computer used during the undercover calls. *See id.*, ¶¶ 14-21.

Logs myself, I found no issues of concern on the system…."[65] Indeed, the FTC undercover computer used during all three undercover calls was free of viruses, spyware, malware, or other security or performance issues at the time of the calls.[66] Defendants' representations about the "Error" and "Warning" messages are false.[67]

b. Defendants use the computer's System Configuration to scare consumers into believing that "Stopped" services are evidence of computer viruses or other problems.

Another trick that Defendants use is to show the computer's System Configuration and claim that problems in the computer have caused a number of Windows services to stop working.[68] For instance, during Call Two, Defendants' telemarketer claimed that the "critical errors and warnings" he found in the Event Viewer had caused the "Stopped" services in System Configuration.[69] He explained, "[B]ecause you are getting these errors and warnings, there are a lot of Microsoft services which are getting stuck day by day,"[70] and added, "I'll have to remove all of these critical errors and warnings, along with that, I have to activate these Microsoft services."[71] In Call Three, Defendants' telemarketer prompted System Configuration, which showed several "Stopped" services, and he claimed that "a small glitch in the registry and some junk files" were causing the computer to run slowly.[72]

---

[65] *Id*., ¶ 31.
[66] *Id*., ¶¶ 10, 13, 22, 30, 41; *see also* PX 28, ¶ 8.
[67] PX 35, Exh. A, ¶ 31; *cf*. PX 44, Attach. A ("[After Defendants' 'repairs,'] [t]he event viewer still has warnings [] which I researched and they are harmless.").
[68] *See* PX 40, Attach A.; PX 42, ¶ 4; PX 44, Attach. A; PX 55, Attach. A; *see also* PX 1, ¶ 60.
[69] PX 1, ¶ 61 & Attach. G (screenshot of "Stopped" services in System Configuration).
[70] PX 1, ¶ 61; *see generally* PX 31, Call Two Tr., 15:19-16:24.
[71] PX 1, ¶ 62.
[72] *Id*., ¶86; *see generally* PX 32, Call Three Tr., 17:14-18:17.

In fact, information about the Microsoft services displayed in System Configuration—including the "Stopped" services—would not indicate a security issue or a computer problem.[73] As Mr. Pomeranz explains, "It is normal for services that are not needed to be in the 'Stopped' state and [this] in no way indicates that there is a problem on the system."[74] Defendants' claims about the "Stopped" services are false.[75]

c. Defendants use the computer's Internet Properties to scare consumers into believing that "Untrusted" and "Fraudulent" certificates are evidence of computer hackers or security breaches.

Defendants also frighten consumers by telling them that there are hackers in their computers.[76] One trick that Defendants use is to show a number of "Untrusted" and "Fraudulent" certificates in the computer's Internet Properties and claim that these are evidence of hacking or security breaches. For example, in Call Two, Defendants' telemarketer opened Internet Properties, highlighted a number of these seemingly problematic certificates,[77] and told the FTC investigator, "These are the security breaches. Can you see that? Fraudulent, untrusted…[you] have a lot of fraud."[78] Then, when the FTC investigator told the telemarketer that he has a Google email account, the telemarketer highlighted on the computer screen a certificate identified as "www.google.com" and labeled as "Fraudulent."[79] While doing this, the telemarketer said that "[G]mail [was] getting a fraudulent [activity] as well because there is no

[73] PX 35, Exh. A, ¶ 29.

[74] *Id.* ("Indeed, if all of the listed services were running at the same time, that would be a problem because the system would run very slowly!").

[75] *Id.*

[76] *See, e.g.*, PX 40, Attach. A; PX 41, Attach. A; PX 43, Attach. A; PX 46, Attachs. A-B; PX 47, Attach. A; PX 48, ¶ 3; PX 49, ¶ 4; PX 51, ¶ 5; PX 52, Attach. A; PX 57, Attach. A; PX 58, ¶ 4; PX 59, Attach. A; PX 60, Attach. A; PX 61, ¶ 5; PX 62, ¶ 5; PX 63, Attach. A; PX 64, Attach. A; PX 65, Attach A; PX 70, Attach. C.

[77] PX 1, ¶ 63 & Attach. H (screenshot of "Untrusted" and "Fraudulent" certificates in Internet Properties); *see generally* PX 31, Call Two Tr., 17:5-18:8.

[78] PX 1, ¶ 63.

[79] *Id.*

securities…. So, we have to fix…all these things from the bottom, along with that, we have to get the security, as well."[80]

Despite their alarming labels, the certificates listed in Internet Properties in no way indicate the presence of hackers or security breaches in the computer; in fact, the certificates are a form of consumer protection designed to prevent computer users from sending their information to untrusted web locations.[81] Defendants' representations about the "Untrusted" and "Fraudulent" certificates are false.[82]

d. Defendants show other areas of the computer to scare consumers into believing that they have computer viruses, spyware, malware, or hackers.

Apart from the Event Viewer and System Configuration, Defendants show other areas of the computer to scare consumers about viruses or other unwanted files in their computers.[83] For example, in Call One, Defendants' telemarketers prompted the computer's Prefetch folder and told the FTC investigator that there was "spam" causing the computer to run slowly.[84] This was false.[85] In Call Two, another telemarketer prompted the computer's Temp folder, clicked on a

[80] *Id*.

[81] PX 35, Exh. A, ¶ 33.

[82] *Id*. ("When the investigator admitted to having a Gmail account, the representative used the untrusted www.google.com certificate to personalize the threat further. The representative's statements are false.").

[83] *See* PX 44, Attach A; PX 45, ¶¶ 6, 8; PX 47, Attach. A; PX 50, Attach. A; PX 53, Attach. A; PX 54, Attach. A; PX 58, ¶ 4; PX 60, Attach. A.

[84] PX 1, ¶ 52. A similar exchange occurred in Call Three. *Id*., ¶ 86.

[85] *See* PX 35, Exh. A, ¶ 30 ("'Spam' is generally defined as unwanted email messages, and this directory has nothing to do with email messages. The Prefetch directory contains cached information designed to help the operating system load programs more quickly. The representative's implication that the files in this directory are somehow making the system run more slowly is clearly false.").

text file, and told the FTC investigator, "You see that these are the viruses, malwares."[86] This, too, was false.[87]

Similarly, Defendants show consumers other aspects of the computer, apart from the certificates in Internet Properties, to convince them that there are hackers in their computers.[88] To heighten consumers' desperation, Defendants told them that the hackers in their systems are stealing their personal information and identities.[89] In some instances, Defendants also showed consumers purported news articles about public figures and famous celebrities, who had been hacked, to drive home their point.[90]

In fact, Defendants' representations about detecting viruses, spyware, malware, and hackers in consumers' computers are simply unlawful misrepresentations. Nevertheless, Defendants engaged in these scare tactics to create a sense of urgency in consumers and ultimately to convince consumers that they needed Defendants' services. In numerous instances, Defendants succeeded.[91]

---

[86] PX 1, ¶ 64.

[87] *See* PX 35, Exh. A, ¶ 34 ("Ironically, this file was an installation log from the Symantec Endpoint Protection Suite. So rather than showing any viruses or malware on the system, the representative was actually displaying proof that software was installed on the system to help protect against these threats. The representative's statements are false.").

[88] *See*, *supra*, Footnote 76.

[89] *See*, *e.g.*, PX 46, Attach. B ("He informed me that numerous hackers had access to all our…credit card numbers, passwords and other information which would allow them to steal our financial accounts."); PX 52, Attach. A ("They…showed me I had a foreign IP address and my identity could be stolen…."); PX 54, Attach. A ("[H]e had my personal information on [the screen]…. [H]e said I got this information and that is how others can do it."); PX 60, Attach. A ("[They] were telling…that those hackers would be able to access my private information."); PX 64, Attach. A. ("He said my system was so badly compromised that it was a matter of probably days before my entire identity would be stolen.").

[90] PX 41, Attach. A; PX 64, Attach. A.

[91] *See*, *e.g.*, PX 40, Attach. A ("[They] had me convinced that the problem was serious and needed to be resolved ASAP."); PX 43, Attach. A ("[H]e said a hacker had gotten into my system. Panicked, I believe [sic] him…."); PX 45, ¶ 8 ("I am not very computer savvy, so I relied on the representatives statements that I had viruses and that they were removing them from my computer."); PX 49, Attach. A; ("They made it sound really serious and tried to rush me into

One consumer recalled becoming suspicious at first and told the telemarketer, "[M]aybe I should take my computer to an Apple store," but "[t]he representative again said that my computer would not work and I would lose everything if I did not fix it right away…. I felt panicked when he told me that my computer was at risk…. [so] I agreed to pay Uber Tech Support to fix my computer."[92] Another consumer similarly expressed reluctance but was overcome by Defendants' deception: "I said I needed a day or so to think about this…. This male put the fear of God into me as I am not an expert on computers…. He said I couldn't call back a day or so. I agreed to go through with the service."[93]

After convincing consumers that they need Defendants' technical support services, Defendants' telemarketers obtained consumers' payment information, directed consumers to Defendants' website to complete the purchase transactions,[94] and charged consumers hundreds

---

getting the 'hackers' off my 'network.'"); PX 50, Attach. A ("He intimidated me into and conned me into thinking that I was at severe risk for all my devices being compromised."); PX 51, ¶ 6 ("I was naïve but at the same time scared that I was being hacked so I agreed [to buy their services.]"); PX 55, Attach. A ("Panicked, I agreed…. I was hesitant, and he pressured me for my credit card info."); PX 56, ¶¶ 3, 5 ("I am by no means an advanced computer user and was scared that in fact my computer had been infected…."); PX 58, ¶ 4; PX 59, Attach. A ("I wanted to think about it but they scared me by saying these 'outside devices' could do some serious damage."); PX 60, Attach. A ("I was led to believe…that I needed a 'permanent' solution or that I would be at risk of identity theft…."); PX 62, ¶ 8 ("[I] was again presented with the "doomsday scenario" that my computer and router were infected."); PX 63, Attach. A ("It all seemed strange but quite honestly it scared [ ] me…. I was desperate so I agreed."); PX 64, Attach. A; PX 65, Attach A. ("[He] told me…someone hacked into my computer…. Of course, that made me panic."); PX 70, Attach. C ("I in fear reluctantly agreed….").

[92] PX 58, ¶ 4.

[93] PX 64, Attach. A. Even worse, in at least two instances, Defendants' telemarketers refused to relinquish control of the computer to scare consumers into paying for services. *See* PX 54, Attach. A ("I expressed immediate concern which he ignored and continued controlling my PC…. I asked him to release control of my PC. [H]e would not and kept telling me…that I had to pay…. I started [to] X him out of the screens but it wouldn't work."); PX 55, Attach. A ("I told him to stop working on my computer and to refund my money immediately…. They refused my full refund and continued doing things to my computer upon my direction to stop.").

[94] During all three undercover calls, Defendants' telemarketers directed the FTC investigator to www.ubertechsupport.com to complete the order process. *See* PX 1, ¶¶ 53-54,

and even thousands of dollars for a one-time repair and/or for long-term security and support services.[95]

Next, Defendants' telemarketers transferred the remote access session to Defendants' technicians who performed the "repairs."[96] In some instances, Defendants did not fix the real technology issues for which unsuspecting consumers called Defendants.[97] In other instances, it was clear that consumers did not need Defendants' services at all.[98] One consumer recounted, "I knew I had been scammed when I called Best Buy the next day. My computer was new, I'd had it two days. [A] member of Geek Squad told me that no viruses were in the computer. [It] was a 'clean' machine. [There] was no problem, no virus infections, no need for repair."[99]

Similarly, in Call Two, Defendants performed "repair" services that were not needed. For example, Defendants' technician changed the computer's Visual Effects settings and re-set the virtual memory file size. Expert analysis showed that, at the time of the "repair process," the FTC computer had no display performance issues and had substantial available disk space,

---

65-67, 87-88. However, the FTC investigator agreed to purchase services during Call Two only. *See* PX 1, ¶¶ 65-67.

[95] *See, e.g.*, PX 40, Attach. A (charged $499); PX 42, ¶ 5 ($2,797); PX 43, Attach. A ($1,700); PX 44, Attach. A ($599); PX 45, ¶ 9 ($999); PX 46, Attach. A ($1,298); PX 47, Attach. A ($499); PX 48, ¶ 3 ($599); PX 50, Attach. A ($2,396); PX 51, ¶ 6 ($2,295); PX 52, Attach. A ($299); PX 53, Attach. A ($328); PX 55, Attach. A ($798); PX 56, ¶ 5 ($199); PX 57, Attach. A. ($498); PX 58, ¶ 6 ($299); PX 59, Attach. A ($999); PX 60, Attach. A ($2,498); PX 61, ¶ 6 ($1,998); PX 62, ¶ 6 ($799); PX 63, Attach. A ($428); PX 64, Attach. A ($477.99); PX 65, Attach A. ($299); PX 66, p. 3 ($499); PX 69, ¶ 7 ($299); PX 70, Attachs. B-C ($1,397); *see also* PX 1, ¶ 73 ($199).

[96] *See, e.g.*, PX 1, ¶ 73.

[97] *See, e.g.*, PX 40, Attach. A; PX 43, Attach. A; PX 46, Attachs. A-B; PX 51, ¶ 7; PX 57, Attach. A; PX 59, Attach. A; PX 60, Attach. A; PX 64, Attach. A.

[98] *See, e.g.*, PX 49, ¶ 4 ("When I later spoke to an actual Apple representative, the representative told me that it…the issue was with my TV, not my computer."); PX 52, Attach. A ("The next day I called my Century link DSL provider and they assured me that…I DID not have a foreign IP address on my computer."); PX 53, Attach. A; PX 57, Attach. A. ("[A]fter working with the real Apple, I was informed there was no one trying to break into my computer…."); PX 59, Attach. A ("I never had any problems with my computer only my printer….Bottom line there never was anything wrong with my computer.").

[99] PX 53, Attach. A.

rendering these actions unnecessary.[100] Next, the technician removed the security suite already installed on the FTC computer and replaced it with a different security program, which is functionally equivalent and provides "no improvement in the security of the system"[101]—yet another unnecessary action.

Even worse, some of Defendants' actions during the "repair process" had a negative impact on the FTC computer's performance and security. For example, Defendants' technician deleted the files in the Prefetch folder, which would cause computer applications to launch "slightly slower."[102] Next, the technician uninstalled the computer's Mozilla Maintenance Service program, which prevents automatic updates—including security fixes—to the Firefox web browser.[103] Finally, the technician disabled several types of important operating system warnings, including warnings about virus protection and automatic updates to the computer's operating system.[104] This "hurts the overall security of the operating system."[105]

Based on Mr. Pomeranz's analysis of Defendants' representations and actions during the undercover calls, he opines, "Despite the representatives' claims to the contrary, there were no security issues with the investigator's PC at the time of the undercover calls. Given this fact, none of these actions were necessary."[106] Regarding Defendants' specific actions in Call Two,

---

[100] PX 35, Exh. A, ¶¶ 41-42, 44.

[101] *Id.*, ¶ 47 ("The customer paid for a product that he did not need and which does not make his system any more secure than it was prior to the call."); *cf*. PX 51, ¶ 6; PX 52, Attach. A; PX 63, Attach A; PX 69, p. 3.

[102] PX 35, Exh. A, ¶ 45. In some instances, Defendants deleted consumers' important programs and files. *See, e.g*., PX 44, Attach. A ("My Wondershare software was completely deleted w/all my projects!!!); PX 63, Attach. A ("Later I found out that they deleted my entire list of business phone numbers.").

[103] PX 35, Exh. A, ¶ 46 ("[D]isabling the automatic update feature for Firefox hurts the overall security of the system rather than enhancing it.").

[104] *See* Compl., Attachs. E-F (screenshots of technician disabling the important warnings).

[105] PX 35, Exh. A, ¶ 48.

[106] *Id*., ¶ 13.

he adds, "It is worth noting again that these 'cleanup' tasks were unnecessary on the investigator's newly installed, already clean system."[107]

Consumers, who later realize they were scammed by Defendants, have had to expend additional time and money to get their computers examined by a legitimate company, remove any programs that Defendants installed, or purchase new devices altogether out of fear or insecurity from their experience with Defendants.[108]

C. Individual Defendants Are Personally and Extensively Involved in Defendants' Deceptive Scheme.

1. Defendant Bruce Bartolotta is personally and extensively involved in the scheme.

Defendant Bartolotta is an owner, officer, and registered agent of C4S-CT and is an owner, chief financial officer, secretary, director, and registered agent of Innovazion.[109] Through Innovazion, he owns iSourceUSA.[110] In addition to the authority and responsibilities inherent in his positions, Bartolotta is extensively involved in Defendants' (1) banking and finances, (2) telephone and website services, and (3) consumer complaint handling.

Bartolotta is involved in Defendants' banking and finances. He has access to at least one bank account held in the name of Innovazion that Defendants use.[111] Bank statements show that iSourceUSA and Spanning Source deposited hundreds of thousands of dollars into this account on multiple occasions.[112] They also show transfers of substantial funds from this account to at

[107] PX 35, Exh. A, ¶ 39.
[108] *See* PX 43, Attach. A; PX 45, ¶ 11; PX 49, Attach. A; PX 49, Attach. A; PX 52, Attach. A; PX 53, Attach. A; PX 54, ¶ 4; PX 58, ¶ 10; PX 60, Attach. A; PX 62, ¶ 11; PX 65, Attach A.
[109] *See, supra*, Section II.B.
[110] *Id.*
[111] PX 1, ¶ 9.
[112] *Id.*

least one foreign entity associated with Innovazion's vice president.[113] Further, the statements show that this account has been used to pay for business expenses related to, among other things, website services (*i.e.*, GoDaddy.com), remote-access services (*i.e.*, LogMeIn.com), as well as payments to third parties made by Bartolotta himself.[114]

Bartolotta has applied for and obtained at least one merchant payment processing account ("merchant account") for Innovazion, even personally guaranteeing the account.[115] A merchant account is essential to any business that wants to accept and process card payments; indeed, without it, Defendants could not have charged consumers' credit or debit cards. The bank opened the merchant account on November 19, 2014, but terminated it shortly thereafter, on December 10, 2014, because Innovazion was placed on MasterCard's MATCH System.[116]

Bartolotta is also involved in Defendants' telephone services. Either personally or through his employees, Bartolotta has registered to use, paid for, and managed Defendants' telephone services, including the telephone numbers listed conspicuously on Defendants' main business websites,[117] provided to consumers as call-back numbers,[118] and those numbers where

[113] *See* PX 1, ¶ 9. The bank statements show that funds were wired from this account to "innovazion research t ltd." *Id.* The FTC believes that this refers to Innovazion Research Private Limited, an Indian entity associated with Innovazion's vice president. *See* PX 15; PX 26. Indeed, additional evidence demonstrates Defendants' history of transferring substantial amounts of money to this entity on a frequent basis. *See, infra,* Section III.F.

[114] *See* PX 1, ¶ 9.

[115] *See* PX 6, pp. 3-10.

[116] *See id.*, p. 1. A merchant is placed on MasterCard's MATCH System for several different reasons, including "Excessive Chargebacks" and "Excessive Fraud," among others. *See* "Security Rules and Procedures – Merchant Edition (30 July 2015)," pp. 100-09, available at https://www.mastercard.us/en-us/about-mastercard/what-we-do/rules.html (last viewed Oct. 10, 2015). Generally, the merchant is made aware of the problem, such as excessive chargebacks, in order to give the merchant an opportunity to correct the problem and avoid being placed on the MATCH System.

[117] *See* PX 17; PX 18; PX 19; PX20.

[118] *See, e.g.*, PX 1, ¶ 81; PX 48, Attach B; PX 70, Attach. D.

consumers' calls are ultimately forwarded.[119] Evidence shows that Bartolotta and at least one employee control and pay for the use of these telephone numbers[120] and that Defendants are continuing to use them to solicit consumers.[121]

Bartolotta is further involved in Defendants' website services. Through his company, Innovazion, Bartolotta has registered to use, paid for, and managed Defendants' business websites. These include Defendants' main consumer-facing websites, www.click4support.net, www.click4support.com, www.c4sts.com, and www.ubertechsupport.com.[122] These also include www.c4s.us,[123] which Defendants have used to gain remote access to consumers' computers, and www.tekdex.com,[124] which is purportedly an online "Helpdesk" for Defendants' existing customers.[125] Evidence shows that Defendants are currently using these business websites and that they intend to continue using at least some of them well into the future.[126]

In addition to managing Defendants' money and operational needs, Bartolotta has handled consumer complaints lodged against Defendants, in turn, giving him direct knowledge of Defendants' unlawful business practices. As C4S-CT's "VP Marketing" and "complaint handler,"[127] he has received all consumer complaints filed through the BBB since at

---

[119] *See* PX 1, ¶ 12.

[120] *See* PX 9, pp. 1-32.

[121] *See* PX 1, ¶ 12.

[122] *See id.*, ¶ 19; PX 23; *see also* PX 10; PX 11, GD 000139-143, 354-355, 1016, 1048; PX 12, WWD 000001-4, 114.

[123] PX 22 (copy of www.c4s.us captured on Apr. 21, 2015); *see also* PX 54, Attach. A.

[124] PX 21; *see also* PX 1, Attachs. P-Q.

[125] *See* PX 1, ¶ 19; PX 23; *see also* PX 11, GD 000139-143, 205, 293-295, 1017-1018, 1023, 1067, 1073, 1126.

[126] *See, e.g.*, PX 11, GD 000140 (www.tekdex.com active until April 11, 2017); PX 11, GD 000142 (www.c4s.us active until March 23, 2017); PX 11, GD 000143 (www.ubertechsupport.com active until April 15, 2016); PX 11, GD 000142 (www.c4sts.com active until November 6, 2015).

[127] PX 67, ¶¶ 8, 10-11. In addition to Bartolotta, the BBB sends a copy of each consumer complaint to admin@click4support.net and george@click4support.net, an email address used by Defendant Saab. *Id.*, ¶ 10; *see also* PX 14 (complaint-related correspondence by Saab).

least 2013.[128] These complaints describe in detail consumers' experiences with Defendants' scheme. Throughout the complaint process, Bartolotta remains the main contact with the BBB and receives all related correspondence, including communications from consumers.[129]

2. Defendant George Saab is personally and extensively involved in the scheme.

Defendant Saab is an owner and officer of iSourceUSA and Spanning Source and is a business manager of C4S-CT.[130] In addition to the authority and responsibilities inherent in his positions, Saab's broad involvement includes Defendants' (1) banking and finances, (2) consumer complaint handling, and (3) and office leasing.

Saab is involved in Defendants' banking and finances. He is an authorized signer for multiple Spanning Source bank accounts, at times signing his name as the company's "President," "Founding Partner," and "Managing Member/Partner."[131] He is also an authorized signer for a number of iSourceUSA bank accounts, at times signing his name as a "Managing Member/Partner."[132] As an authorized signer, Saab has significant control over the movement of Defendants' funds in and out of these accounts.[133]

Either on his own or with others, Saab has applied for and obtained merchant accounts for Spanning Source. In June 2012, Saab obtained a merchant account for Spanning Source that eventually allowed Defendants to process millions of dollars in consumer payments.[134] In February 2014, Saab applied for another merchant account for Spanning Source with a different

[128] *See* PX 67, ¶¶ 8, 10-11.
[129] *Id*., ¶¶ 10-11.
[130] *See, supra,* Section II.B.
[131] PX 7, pp. 5-15, 27-29.
[132] PX 6, pp. 42-43; PX 7, pp. 1-4, 16-26.
[133] *See, e.g.,* PX 7, p. 27.
[134] *Id*., pp. 30-33; *see also* PX 1, ¶ 10.

bank, designating himself as the authorized signer for the account and using an iSourceUSA account as the payment source.[135]

In addition to controlling the money, Saab has handled and resolved consumer complaints filed against Defendants, which has provided him with extensive insight into Defendants' unlawful business practices. He is a "Customer Service Manager" for C4S-CT[136] and is a manager and complaint handler for iSourceUSA and Spanning Source.[137] In these roles, he receives and reviews consumer complaints forwarded by the BBB.[138] In a number of instances, he has personally communicated with individual consumers by telephone and email about their complaints.[139] He has also communicated directly with the BBB regarding consumer complaints.[140] Saab has the authority to approve consumer refunds and, in some instances, has responded directly to consumers' refund requests.[141] When a complaint was resolved, he notified the BBB to close the complaint.[142]

Saab is also involved in Defendants' office leasing. In April 2015, Defendants listed Saab as the lease manager for a virtual office in Newtown, Pennsylvania that iSourceUSA and

---

[135] *See* PX 6, p. 41; *see also* PX 7, pp. 22-24. In the same month, Saab was listed as the business contact person in Spanning Source's application for yet another merchant account, which eventually allowed Defendants to process millions of dollars in consumer payments. *See* PX 6, pp. 11-14; *see also* PX 1, ¶ 9.

[136] PX 67, ¶ 10; *see also* PX 14 (complaint-related correspondence by Saab).

[137] *See* PX 68, Goode Decl., ¶¶ 5, 12; *see also* PX 13 (complaint-related correspondence by Saab).

[138] *See* PX 67, ¶ 10; *see also* PX 14.

[139] *See* PX 14. In at least one instance, Saab lied about his company's affiliation with a legitimate U.S. company. *Compare* PX 14, pp. 12-13 ("We do support AT&T as well as many other technology products.") *with* PX 37, ¶ 5 (stating that AT&T has "no contracts with any [of the Corporate Defendants.]").

[140] *See* PX 13; PX 14.

[141] *See* PX 14.

[142] *Id*.

Spanning Source use.[143] The lease indicates that Defendants intend to use this virtual office until at least April 30, 2016.[144]

3. Defendant Chetan Bhikhubhai Patel is personally and extensively involved in the scheme.

Defendant C. Patel is an owner and officer of iSourceUSA and Spanning Source.[145] Apart from the authority and responsibilities inherent in his positions, C. Patel is extensively involved in Defendants' (1) banking and finances, (2) website services and office leasing, and (3) consumer complaints handling.

C. Patel is involved in Defendants' banking and finances. He is an authorized account signer for a number of Spanning Source and iSourceUSA bank accounts, at times signing his name as a "Managing Member/Partner."[146] Like Saab, C. Patel has extensive control over the movement of Defendants' money in and out of these accounts.[147]

C. Patel has applied for and obtained at least one merchant account for Spanning Source, also personally guaranteeing the account.[148] Through this single merchant account alone, Defendants processed $8,693,157 in gross sales from 22,862 sales transactions during February to November of 2014.[149] The bank terminated this merchant account in November 2014 due to excessive chargebacks.[150]

As part of the application for this account, C. Patel submitted statements for another merchant account that Defendants used in 2013 and 2014. Those statements show that Defendants processed $7,092,638 in gross sales (27,329 sales transactions) during January to

[143] *See* PX 8; PX 25.
[144] PX 8.
[145] *See, supra,* Section II.B.
[146] *See, supra,* Footnotes 131-32.
[147] *See, e.g.,* PX 7, p. 27.
[148] PX 6, pp. 11-40.
[149] PX 1, ¶ 9.
[150] PX 6, p. 1.

December of 2013 and $1,639,786 (4,503 sales transactions) in January 2014.[151] Visa red-flagged this merchant account as early as December 2013 for excessive chargebacks.[152]

C. Patel is also involved in Defendants' website services, office leasing, and handling of consumer complaints. He is listed as a registrant of www.click4support.com, one of Defendants' main consumer-facing websites.[153] In April 2015, he entered into the lease of the virtual office that Spanning Source and iSourceUSA use.[154] Further, through Saab, C. Patel keeps apprised of at least some consumer complaints and related correspondence forwarded by the BBB.[155]

4. Defendant Niraj Patel is personally and extensively involved in the scheme.

Defendant N. Patel is an owner and officer of iSourceUSA and Spanning Source.[156] In addition to the authority and responsibilities inherent in his positions, he is an authorized account signer for multiple Spanning Source bank accounts, at times signing his name as the company's "President," "Vice president," and "Managing Member/Partner."[157] He is also an authorized account signer for multiple iSourceUSA bank accounts, at times signing his name as a "Managing Member/Partner."[158] Much like Saab and C. Patel, N. Patel has broad control over the flow of Defendants' money in and out of these accounts. N. Patel is also involved in Defendants' office leasing. He pays for the virtual office that Spanning Source and iSourceUSA use.[159]

---

[151] PX 1, ¶ 9.
[152] PX 5, VISA 00010-18 (shows monthly chargeback rates from November 2013 to February 2014 were 3.68%, 5.07%, 6.05%, and 20.63%, respectively).
[153] PX 10.
[154] PX 8.
[155] *See, e.g.*, PX 14, pp. 25-26.
[156] *See, supra*, Section II.B.
[157] *See, supra*, Footnote 131.
[158] *See, supra*, Footnote 132.
[159] *See* PX 8; PX 25.

D. Corporate Defendants Operate as a Common Enterprise.

Defendants C4S-CT, iSourceUSA, Innovazion, and Spanning Source have operated as a common enterprise while engaging in the illegal acts and practices described above. As detailed above, Defendants have conducted their business practices through an interrelated network of companies that have common or shared (1) owners, officers, and employees,[160] (2) office locations and business addresses,[161] and (3) business websites, telephone numbers, and telemarketers used to solicit consumers.[162] Defendants share at least one bank account,[163] and Saab has authorized refunds to customers of iSourceUSA and C4S-CT.[164]

The FTC investigator's experience with Defendants during his undercover calls encapsulates Defendants' interrelatedness. In Call Two, while being directed to pay for services, the FTC investigator questioned Defendants' telemarketer about the connection between Click4Suport and Uber Tech Support.[165] The telemarketer simply explained, "[I]t's the one and the same thing…. Uber Tech Support…is the same as the Click4Support."[166]

E. Defendants Attempt to Conceal Their Identity to Perpetuate Their Scheme.

Apart from the calculated lies regarding their affiliation with legitimate U.S. companies, Defendants have undertaken deliberate steps to confuse consumers and to evade law enforcement. As detailed above, Defendants have used multiple company names, business websites, telephone numbers, and addresses.[167] Indeed, in addition to those already discussed, Defendants have used other fictitious names and websites to trick even more consumers into

---

[160] *See, supra*, Section II.B.
[161] *Id.*
[162] *See, supra*, Section III.A-C.
[163] *See, supra*, Section III.C.1.
[164] *Id.*; *see also* PX 14; PX 50; PX 59.
[165] PX 1, ¶ 66.
[166] *Id.*, ¶¶ 66-67. A similar exchange occurred in Call Three. *Id.*, ¶ 88.
[167] *See, supra*, Sections II.B, III.B-C.

paying for unnecessary technical support services. For example, Defendants have also operated as "Click4Fix" and "CleanAndFastPC"[168] using the websites www.click4fix.net[169] and www.cleanandfastpc.com.[170] Defendants own and operate these two websites.[171] Both list the same telephone number listed in www.click4support.com and www.c4sts.com, thus funneling consumers to the same group of Defendants' telemarketers and "technicians."[172] Financial statements show that Click4Fix generated over $20.3 million in gross revenues during 2012 through 2014.[173]

Defendants have also taken steps to minimize information about them that is available to the public. For example, they registered their newest website, www.ubertechsupport.com, with a privacy protection service, making it impossible for consumers to learn who is responsible for the website.[174] On at least two separate occasions, Saab falsely denied to the BBB the connection between C4S-CT and iSourceUSA.[175] BBB records show that, beginning in February 2015, Defendants stopped responding to consumer complaints and ignored refund requests; in fact, Defendants have never responded to complaints filed against Uber Tech Support.[176] On September 22, 2015, a representative of C4S-CT logged into the BBB business portal and removed the publicly-viewable legal name of the company and two business contacts.[177]

---

[168] Spanning Source has also used the fictitious name "Live Tech Help," and iSourceUSA has also used "Security Square" and "Support Square." PX 7, pp. 14-18, 25-26.

[169] PX 33 (copy of www.click4fix.net captured on June 18, 2015).

[170] PX 34 (copy of www.cleanandfastpc.com captured on June 18, 2015).

[171] PX 11, GD 000140, 142.

[172] *Compare* PX 33, PX 34 *with* PX 17, PX 19.

[173] PX 1, ¶ 9.

[174] PX 23; *see also* PX 1, ¶ 22.

[175] PX 13; PX 14, pp. 25-26.

[176] *See, e.g.*, PX 68, ¶ 12. Based on the FTC's review of complaint files produced by the BBB, it appears that Defendants stopped responding to consumer complaints in February 2015.

[177] *See* PX 67, ¶ 14.

F. The Consumer Injury Inflicted by Defendants is Significant and Ongoing.

During 2013 and 2014, Defendants tricked consumers into paying them $17,900,324.[178] This resulted from 55,966 sales transactions completed within only a 23-month period.[179] These figures were derived from only two of Defendants' merchant accounts, and the FTC believes that Defendants have used other merchant accounts. Therefore, the total consumer injury inflicted by Defendants is likely greater than $17.9 million.[180]

Further, Defendants have a demonstrated history of transferring at least part of their ill-gotten gains overseas.[181] For example, the FTC's forensic accounting analysis shows that, during January 2013 to August 2014, Defendants originated at least 73 wire transfers totaling over $4.6 million to financial institutions in India.[182] The beneficiary of these wire transfers was an Indian entity named Innovazion Research Private Limited.[183]

The FTC has received approximately 444 consumer complaints filed against Defendants, and it continues to receive complaints.[184] The complaints with sufficient details confirm the

---

[178] Defendants processed payments totaling $9,207,167 using one merchant account and $8,693,157 using another merchant account. *See* PX 1, ¶¶ 9-10.

[179] Defendants processed 33,104 sales transactions using one merchant account (during January 2013 to February 2014) and an additional 22,862 sales transactions using another merchant account (during February to November 2014). *See* PX 1, ¶¶ 9-10.

[180] In fact, the FTC knows of at least one bank that Defendants have used to process payments, and the FTC believes that Defendants have processed over $11.7 million (39,986 sales transactions) through this bank during April 2014 to July 2015. *See* PX 1, ¶ 8. The FTC did not request information from this bank because its policy requires the disclosure of such requests to its customers. Such disclosure would have alerted Defendants of the FTC's investigation.

[181] *See* PX 16, George Decl., ¶ 9. Defendants iSourceUSA, Innovazion, and Spanning Source also have a history of transferring funds to each other. During May 2013 to November 2014, approximately $7,010,405 flowed among these entities through 112 transactions. *Id*., ¶ 8.

[182] PX 16, ¶ 9.

[183] *Id*. As noted, Innovazion Research Private Limited is associated with Defendant Innovazion's vice president. *Compare* PX 15 *with* PX 26.

[184] *See, e.g.,* PX 1, ¶ 5 (approximately 266 complaints); PX 67, ¶ 12 (155 complaints); PX 68, ¶¶ 13-14 (23 complaints). To note for the Court, the 266 complaints received by the FTC

pattern of deceptive and unlawful practices that Defendants engage in to induce consumers to pay for Defendants' services.

IV. ARGUMENT

In the interest of immediately protecting consumers, the FTC seeks a TRO, which would temporarily accomplish, among other things, the following: (1) enjoin Defendants from making misrepresentations to consumers; (2) freeze Defendants' assets; (3) appoint a temporary receiver over the Corporate Defendants; (4); allow the temporary receiver and the FTC immediate access to Defendants' business premises; and (5) require Defendants to preserve and produce their business records. As set forth below, the law and the evidence overwhelmingly support the Court's entry of the attached Proposed Temporary Restraining Order ("Proposed TRO").

A. The Court has the Authority to Grant the FTC's Requested Relief.

Section 13(b) of the FTC Act authorizes this Court to grant a permanent injunction to stop violations of "any provision of the law" enforced by the FTC.[185] Specifically, the second proviso of Section 13(b) provides that, "in proper cases the Commission may seek, and after proper proof, the court may issue a permanent injunction."[186] Once the FTC has invoked the equitable power of a federal court, the full breadth of the court's authority is available, including

---

through the FTC's Consumer Sentinel database may include complaints that consumers filed directly with the BBB and other agencies. *See, e.g.*, PX 1, ¶ 5.

[185] 15 U.S.C. § 53(b). The Court has subject matter jurisdiction over the FTC's claims under the FTC Act and TSR. 28 U.S.C. §§ 1331, 1337(a), 1345; 15 U.S.C. §§ 45(a), 53(b), and 1693o(c). Further, the Court has personal jurisdiction over all Defendants pursuant to Section 13(b), which authorizes nationwide service of process. 15 U.S.C. § 53(b); *see also Pinker v. Roche Holdings Ltd.*, 292 F.3d 361, 369 (3rd Cir. 2002) ("[A] federal court's personal jurisdiction may be assessed on the basis of the defendant's national contacts when the plaintiff's claim rests on a federal statute authorizing nationwide service of process."). Moreover, venue is proper in the Eastern District of Pennsylvania, given the Defendants' presence and connections in the district. 28 U.S.C. § 1391(b) and (c); 15 U.S.C. § 53(b).

[186] 15 U.S.C. § 53(b). This action qualifies as a "proper case" because it is appropriate to invoke the remedies of Section 13(b) in cases where there is evidence of routine fraud or a straightforward deceptive practice. *See FTC v. World Travel Vacation Brokers*, 861 F.2d 1020, 1026-28 (7th Cir. 1988).

the power to grant ancillary relief necessary to preserve the possibility of effective final relief.[187] Indeed, "a court's equitable powers assume an even broader and more flexible character when the public interest is involved."[188] Such ancillary relief could include a temporary restraining order and a preliminary injunction that enjoins deceptive and unfair business practices, freezes assets for consumer restitution, appoints a temporary receiver, and allows immediate access to business premises, among other things.[189]

This Court and others in the Third Circuit and throughout the nation have issued the type of preliminary relief the FTC seeks here.[190] This includes courts that have entered TROs in numerous "tech support scam" cases filed by the FTC and its state partners,[191] similar to this action—while helpful to the Court, this fact unfortunately highlights the pervasive and harmful nature of the kind of scam that Defendants operate.[192]

---

[187] *See FTC v. H. N. Singer, Inc.*, 668 F.2d 1107, 1113 (9th Cir. 1982); *In re Nat'l Credit Mgmt. Group, L.L.C.*, 21 F. Supp. 2d 424, 462 (D.N.J. 1998).

[188] *U.S. v. Lane Labs-USA, Inc.*, 427 F.3d 219, 231 (3d Cir. 2005) (quoting *Porter v. Warner Holding Co*., 328 U.S. 395, 398 (1946)).

[189] *See H. N. Singer*, 668 F.2d at 1111-13; *see also, infra,* Footnotes 190-91.

[190] *See, e.g., FTC v. First Consumers, LLC*, No. 2:14-cv-01608-GAM (E.D. Pa. Mar. 18, 2014); *FTC v. NHS Systems, Inc.*, No. 2:08-cv-02215 (E.D. Pa. May 14, 2008); *FTC v. Zuccarini*, No. 2:01-cv-04854 (E.D. Pa. Dec. 21, 2006); *FTC v. Morrone's Water Ice*, No. 2:02-cv-03720 (E.D. Pa. Jun. 18, 2002); *FTC v. United Credit Adjusters, Inc.*, No. 3:09-cv-00798 (D.N.J. Feb. 24, 2009); *FTC v. Dutchman Enterprises, LLC*, No. 2:09-cv-00141 (D.N.J. Jan. 14, 2009); *FTC v. Sparta Chem, Inc.*, No. 2:96-cv-03228 (D.N.J. Nov. 14, 2007); *FTC v. Stafford*, No. 3:05-cv-0215 (M.D. Pa. Feb. 2, 2005); *FTC v. Rann*, No. 3:00-cv-02792 (D.N.J. Jun. 9, 2000); *Nat'l Credit Mgmt.*, 21 F. Supp. 2d at 429 (D.N.J. 1998); *World Travel*, 861 F.2d at 1022; *FTC v. World Wide Factors, Ltd.*, 882 F.2d 344, 346 (9th Cir. 1989); *FTC v. Inc21.com Corp.*, 745 F. Supp. 2d 975, 988 (N.D. Cal. 2010).

[191] *See, e.g., FTC v. Inbound Call Experts, LLC*, No. 14-81395-CIV-MARRA (S.D. Fla. Nov. 14, 2014) (TRO sought by FTC and the State of Florida); *FTC v. Boost Software, Inc*., No. 14-81397-CIV-MARRA (S.D. Fla. Nov. 12, 2014) (same); *FTC v. Pairsys, Inc*., No. 1:14-CV-1192 (N.D.N.Y. Sept. 30, 2014); *FTC v. PCCare247 Inc*., No. 1:12-cv-07189-PAE (S.D.N.Y. Sept. 25, 2012); *FTC v. Pecon Software Ltd*., No. 12-cv-7186-PAE (S.D.N.Y. Sept. 25, 2012); *FTC v. Marczak*, No. 12-cv-7192-PAE (S.D.N.Y. Sept. 25, 2012); *FTC v. Finmaestros, LLC*, No.12-cv-7195-PAE (S.D.N.Y. Sept. 25, 2012); *FTC v. Lakshmi Infosoul Servs. Pvt. Ltd*., No. 12-cv-7191-PAE (S.D.N.Y. Sept. 25, 2012).

[192] *See generally*, "FTC Obtains Court Orders Temporarily Shutting Down Massive Tech

B. The FTC Meets the Requirements to Obtain the Requested Relief.

To obtain a temporary restraining order, the FTC must demonstrate that (1) it is likely to succeed on the merits of its case and (2) the equities favor the granting of preliminary relief.[193] In balancing the equities, the public interest in addressing law violations commands greater weight.[194] Further, unlike private litigants, the FTC does not need to show irreparable injury.[195] Here, the FTC meets both requirements to obtain the Proposed TRO.

1. The FTC demonstrates an overwhelming likelihood of success on the merits, showing that Defendants have violated Section 5(a) of the FTC Act, CUTPA, and Pa UTPCPL (Counts I-II and V-X).

An act or practice is "deceptive" where a material representation, practice, or omission is likely to mislead consumers acting reasonably under the circumstances.[196] A representation is material if it "involves information that is important to…[a] consumer's choice of or conduct regarding a product."[197] Further, "[e]xplicit claims or deliberately-made implicit claims…are presumed to be material."[198] A representation does not have to be made with intent to deceive in

---

Support Scams" (Nov. 19, 2014), www.ftc.gov/news-events/press-releases/2014/11/ftc-obtains-court-orders-temporarily-shutting-down-massive-tech; "At FTC's Request, Court Shuts Down New York-Based Tech Support Scam Business" (Oct. 24, 2014), www.ftc.gov/news-events/press-releases/2014/10/ftcs-request-court-shuts-down-new-york-based-tech-support-scam; "FTC Halts Massive Tech Support Scams" (Oct. 3, 2012), www.ftc.gov/news-events/press-releases/2012/10/ftc-halts-massive-tech-support-scams.

[193] *See, e.g., World Wide Factors*, 882 F.2d at 346 ("Pursuant to 15 U.S.C. § 53(b), the district court is required (i) to weigh equities; and (ii) to consider the FTC's likelihood of ultimate success before entering a preliminary injunction.").

[194] *Id.* at 347.

[195] *Id.* at 346-47; *Nat'l Credit Mgmt.*, 21 F. Supp. 2d at 439-40 (citing *United States v. Richlyn Labs., Inc.*, 827 F. Supp. 1145, 1150 (E.D. Pa. 1992)).

[196] *See Beneficial Corp. v. FTC*, 542 F.2d 611, 617 (3d Cir. 1976); *NHS Sys.*, 936 F. Supp. 2d 520, 531 (E.D. Pa. 2013); *Nat'l Credit Mgmt.*, 21 F. Supp. 2d at 441 (extending application beyond affirmative representations to "omissions or practices").

[197] *FTC v. Bronson Partners, LLC*, 564 F. Supp. 2d 119, 135 (D. Conn. 2008).

[198] *NHS Sys.*, 936 F. Supp. 2d at 531 (citing *Nat'l Credit Mgmt.*, 21 F. Supp. 2d at 441).

order to be deceptive.[199] In determining whether a reasonable consumer would likely rely on stated claims, a court may make a common-sense interpretation of the claims and must judge them from the standpoint of their overall net impression.[200] Moreover, proof of reliance by each consumer misled by Defendants is not required; rather, a "presumption of actual reliance arises once the Commission has proved that the defendants made material misrepresentations, that were widely disseminated, and that consumers purchased the defendant's products."[201]

In numerous instances, Defendants made two kinds of representations to consumers: first, that they are part of or affiliated with well-known U.S. technology companies;[202] second, that they have detected security or performance issues on consumers' computers, including viruses, spyware, malware, or the presence of hackers.[203]

These representations are material. First, Defendants made them expressly to consumers after luring them into calling Defendants' telemarketers.[204] Further, the representations tricked consumers into allowing Defendants to remotely access their computers—in turn, giving Defendants the opportunity to unleash their scare tactics—and, ultimately, the representations induced consumers into paying for technical support services that they did not need.[205] Indeed, it is difficult to imagine that a consumer would purchase Defendants' services had Defendants been truthful about the fact that they are not part of or affiliated with legitimate companies or the

---

[199] *Beneficial Corp.*, 542 F.2d at 617; *NHS Sys.*, 936 F. Supp. 2d at 531; *Nat'l Credit Mgmt.*, 21 F. Supp. 2d at 441.

[200] *See Beneficial Corp.*, 542 F.2d at 617; *Nat'l Credit Mgmt.*, 21 F. Supp. 2d at 441; *FTC v. Davison Assocs.*, 431 F. Supp. 2d 548, 559-60 (W.D. Pa. 2006).

[201] *FTC v. Figgie Int'l*, 994 F.2d 595, 605 (9th Cir. 1993).

[202] *See, supra*, Section III.B.1.

[203] *See, supra*, Section III.B.2.

[204] *See, supra*, Section III.B; *see also NHS Sys.*, 936 F. Supp. 2d at 531; *Nat'l Credit Mgmt.*, 21 F. Supp. 2d at 441.

[205] *See, supra*, Section III.B; *see also FTC v. Bronson Partners, LLC*, 564 F. Supp. 2d 119 (D. Conn. 2008).

fact that they had no idea whether the consumer's computer had viruses, spyware, malware, or hackers.

Finally, these representations are likely to mislead consumers acting reasonably under the circumstances. As detailed above and in a number of sworn declarations, consumers reasonably believed that they were speaking with representatives of legitimate companies who they could trust.[206] This resulted from Defendants' internet ads and popups and their subsequent representations to consumers.[207] Further, consumers reasonably believed that their computers were infected or otherwise compromised due to Defendants' claims and accompanying use of the Event Viewer, System Configuration, Internet Properties, and other areas of the computer.[208]

Therefore, Defendants have committed deceptive acts and practices in violation of Section 5(a) of the FTC Act, as alleged in Counts I and II of the Complaint. These acts and practices also violate CUTPA and Pa UTPCPL, as alleged in Counts V through X.

2. The FTC demonstrates an overwhelming likelihood of success on the merits, showing that Defendants have violated the TSR and Pa UTPCPL (Counts III, IV, and XI).

The TSR prohibits any seller or telemarketer from making a false or misleading statement to induce any person to pay for goods or services.[209] As explained above, Defendants lured consumers into calling Defendants' telemarketing representatives,[210] and then they falsely claimed that they are part of or affiliated with well-known U.S. technology companies[211] and that they have detected security or performance issues on consumers' computers.[212]

---

[206] *See, supra*, Section III.B.1.
[207] *See, supra*, Section III.A-B.1.
[208] *See, supra*, Section III.B.2.
[209] *See* 16 C.F.R. § 310.3(a)(4); *see also* 16 C.F.R. § 310.2(aa), (cc), and (dd) (defining "seller," "telemarketer," and "telemarketing," respectively).
[210] *See, supra*, Section III.A.
[211] *See, supra*, Section III.B.1.
[212] *See, supra*, Section III.B.2.

Defendants made these claims to induce consumers to purchase technical support services, and in numerous instances, they successfully bilked consumers out of hundreds or thousands of dollars.[213] Therefore, Defendants are sellers or telemarketers engaged in telemarketing, and through their acts and practices, have violated the TSR,[214] as alleged in Counts III and IV of the Complaint. These acts and practices also violate Pa UTPCPL,[215] as alleged in Count XI.

3. The balance of equities favors the issuance of the Proposed TRO.

When balancing the equities, "the public interest should receive greater weight" than a litigant's private interest.[216] Indeed, "the public interest in preserving the illicit proceeds…for restitution to the victims is great."[217] This particular interest is implicated when litigants are likely to dissipate assets, and it is a "prime concern" when there is a likelihood that the litigants have violated the FTC Act through deceptive practices.[218] Further, litigants have no legitimate interest in continuing to operate an unlawful enterprise. They "do not have the right to persist in conduct that violates Federal or state law,"[219] and "there is no oppressive hardship to defendants in requiring them to comply with the FTC Act, refrain from fraudulent representation or preserve

---

[213] *See, supra*, Section III.B.2.

[214] A violation of the TSR is also a violation of Section 5(a) of the FTC Act. *See* 15 U.S.C. §§ 57a(d)(3), 6102(c).

[215] Pennsylvania's Telemarketer Registration Act ("Pa TRA"), 73 Pa. Cons. Stat. Ann. § 2241, *et seq.*, prohibits sellers or telemarketers engaged in telemarketing from committing any deceptive or abusive telemarketing acts or practices in violation of the TSR. *See* 73 Pa. Cons. Stat. Ann. § 2245(a)(9). A violation of the Pa TRA is a violation of the Pa UTPCPL. *See* 73 Pa. Cons. Stat. Ann. § 2246.

[216] *World Wide Factors*, 882 F.2d at 347 (citing *FTC v. Warner Commc'ns Inc.*, 742 F.2d 1156, 1165 (9th Cir. 1984)); s*ee also Nat'l Credit Mgmt.*, 21 F. Supp. 2d at 460 (court should accord "greater weight to the public interest").

[217] *FTC v. Affordable Media, LLC*, 179 F.3d 1228, 1236 (9th Cir. 1999); *accord CFTC v. American Metals Exch. Corp.*, 991 F.2d 71, 79 (3d Cir. 1993) (affirming asset freeze "designed to preserve the *status quo* by preventing the dissipation and diversion of assets" until the district court can determine amount of unlawful proceeds).

[218] *See FTC v. Equinox Int'l Corp.*, No. CV-S-99-0969-JBR (RLH), 1999 U.S. Dist. LEXIS 19866, at *28 (D. Nev. Sept. 14, 1999).

[219] *Nat'l Credit Mgmt.*, 21 F. Supp. 2d at 461.

their assets from dissipation or concealment."[220] Indeed, "a court of equity is under no duty to protect illegitimate profits or advance business which is conducted [illegally]."[221]

On one hand, the public interest in stopping Defendants' unlawful conduct and preserving assets to enable this Court to enter effective final relief carries great weight. The evidence demonstrates that Defendants have taken millions of dollars from tens of thousands of consumers through sheer deception.[222] It also shows that Defendants are continuing to do this with deliberate guile,[223] causing ongoing consumer harm, while also shielding their ill-gotten gains offshore.[224] On the other hand, Defendants have no legitimate interest in continuing their fraudulent enterprise, and this Court is under no duty to "protect [Defendants'] illegitimate profits or advance [their] business."[225] Therefore, the balance of equities favor the issuance of the Proposed TRO.

4. The Corporate Defendants operate as a common enterprise and are therefore jointly and severally liable for each other's law violations.

Corporate Defendants C4S-CT, iSourceUSA, Innovazion, and Spanning Source operate as a common enterprise and therefore are jointly and severally liable for each other's violations of the FTC Act, TSR, CUTPA, and Pa UTPCPL.

Companies that take part in a common enterprise are jointly and severally liable for each other's unlawful acts and practices.[226] To determine whether a common enterprise exists, courts consider a number of factors, including: (1) whether business is transacted through a maze of interrelated companies, (2) common control over the business, (3) shared officers and

[220] *World Wide Factors*, 882 F.2d at 347.
[221] *CFTC v. British Am. Commodity Options Corp*., 560 F.2d 135, 143 (2d Cir. 1977) (internal quotes omitted).
[222] *See, supra*, Section III.A-B, F.
[223] *See, supra*, Section III.E.
[224] *See, supra*, Section III.F.
[225] *British Am.*, 560 F.2d at 143.
[226] *See NHS Sys.*, 936 F. Supp. 2d at 533.

employees, (4) shared offices, (5) shared advertising and marketing, (6) commingling of funds, and (7) evidence which reveals that no real distinction existed between the companies.[227] "Inasmuch as no one factor is controlling, courts must consider 'the pattern and frame-work of the whole enterprise….'"[228]

As detailed above, Defendants C4S-CT, iSourceUSA, Innovazion, and Spanning Source have conducted their business through a network of interrelated companies that have common or shared (1) owners, officers, and employees, (2) office locations and business addresses, (3) business websites, telephone numbers, and telemarketers used to solicit consumers, and (4) bank accounts and commingled funds.[229] Therefore, these Corporate Defendants are jointly and severally liable for each other's law violations.

5. The Individual Defendants are personally liable for injunctive and monetary relief.

Individual Defendants Bartolotta, Saab, C. Patel, and N. Patel are liable for their own violations of the FTC Act as well as the Corporate Defendants' unlawful practices.

An individual defendant is personally liable for injunctive and monetary relief based on corporate violations of the FTC Act if "(1) he participated directly in the deceptive acts or had the authority to control them and (2) he had knowledge of the misrepresentations, was recklessly indifferent to the truth or falsity of the misrepresentation, or was aware of a high probability of

[227] *See NHS Sys.*, 936 F. Supp. 2d at 533; *FTC v. Wash. Data Res*., 856 F. Supp. 2d 1247, 1271 (M.D. Fla. 2012) ("If the structure, organization, and pattern of a business venture reveal a 'common enterprise' or a 'maze' of integrated business entities, the Federal Trade Commission Act disregards corporateness.").

[228] *FTC v. Consumer Health Benefits Assoc*., 10-CV-3551 (ILG), 2011 U.S. Dist. LEXIS 92389, at *15-16 (E.D.N.Y. Aug. 2, 2010) (quoting *Del. Watch Co. v. FTC*, 332 F.2d 745, 746 (2d Cir. 1964) (per curiam)).

[229] *See, supra*, Section III.D.

fraud along with an intentional avoidance of the truth."[230] Authority to control the deceptive acts can be demonstrated by the individual's active involvement in corporate affairs, establishment of corporate policy, or assumption of the duties of a corporate officer.[231] Further, an individual's status as a corporate officer gives rise to a presumption of control in a small, closely held company.[232] An individual's knowledge may be shown by "evidence that he or she knew or should have known of the material representations or awareness of a high probability of fraud with intentional avoidance of the truth."[233] "The degree of the defendant's participation in business affairs is probative of his knowledge" of the material misrepresentations.[234] Proof that the individual intended to defraud consumers is not necessary.[235]

Here, each Individual Defendant is a corporate officer of at least two of the Corporate Defendants involved in the common enterprise, and each has the authority to sign documents on behalf of those entities; thus, each has the authority to control the Corporate Defendants. Further, each Individual Defendant is deeply involved in the companies' business affairs. Bartolotta obtained a merchant account which was eventually terminated because Innovazion

---

[230] *NHS Sys.*, 936 F. Supp. 2d at 533-34. Individual liability for monetary relief based on corporate violations requires proof of both elements. *See id*. at 533-35. However, individual liability for injunctive relief requires only a showing of the first of these two elements. *See FTC v. Publ'g Clearing House, Inc*., 104 F.3d 1168, 1170 (9th Cir. 1997); *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104, 1117 (S.D. Cal. 2008). Here, the evidence shows that both elements are met.

[231] *NHS Sys*., 936 F. Supp. 2d at 534; *see also Neovi*, 598 F. Supp. 2d at 1117 (authority to control can also be shown by the individual's "authority to sign documents on behalf of the corporate defendant").

[232] *See, e.g., FTC v. Transnet Wireless Corp.*, 506 F. Supp. 2d 1247, 1270 (S.D. Fla. 2007).

[233] *NHS Sys*., 936 F. Supp. 2d at 534.

[234] *Id*.; *see also FTC v. Amy Travel Serv., Inc*., 875 F.2d 564, 574 (7th Cir. 1989).

[235] *See NHS Sys*., 936 F. Supp. 2d at 534; *Transnet Wireless*, 506 F. Supp. 2d at 1270 ("The knowledge component does not require proof of a subjective intent to defraud; it may be satisfied by a showing of 'actual knowledge of material misrepresentations, reckless indifference to the truth or falsity of such misrepresentations, or an awareness of a high probability of fraud along with an intentional avoidance of the truth.'") (quoting *Amy Travel*, 875 F.2d at 574).

was placed on MasterCard's MATCH System.[236] Moreover, as the designated complaint handler with the BBB since 2013, Bartolotta had direct knowledge of consumers' experiences with Defendants' unlawful practices.[237] Similarly, Saab was the business contact person for a merchant account that was eventually terminated due to excessive chargebacks, a process through which he would have been made aware of a high probability of Defendants' problematic practices, at the least.[238] Saab was also a complaint handler with the BBB, and in many instances, he personally contacted consumers about their complaints.[239] Likewise, C. Patel obtained or had access to at least two merchant accounts, which were both terminated due to excessive chargebacks.[240] Through Saab, C. Patel keeps apprised of at least some consumer complaints and related correspondence forwarded by the BBB.[241] Finally, like the rest of his cohorts, N. Patel is significantly involved in the finances of their fraudulent enterprise.[242] In short, the evidence demonstrates that each Individual Defendant either had actual knowledge of Defendants' unlawful practices or were at least aware of a high probability of fraud while intentionally avoiding the truth. Therefore, these Individual Defendants are liable for injunctive and monetary relief.

---

[236] *See, supra*, Section III.C.1.; *see also, supra*, Footnote 116.

[237] *See, supra*, Section III.C.1.

[238] *See, supra*, Section III.C.2. Before a merchant account is terminated due to excessive chargebacks, the merchant could be placed in a chargeback monitoring program and be required to provide detailed information about its business and its action plan to reduce its chargebacks. *See, e.g.*, "Security Rules and Procedures – Merchant Edition (30 July 2015)," pp.53-57, available at https://www.mastercard.us/en-us/about-mastercard/what-we-do/rules.html (last viewed Oct. 10, 2015) (describing MasterCard's "Excessive Chargeback Program"); "Visa Core Rules and Visa Product and Service Rules (15 April 2015)," pp. 499-500, available at https://usa.visa.com/dam/VCOM/download/about-visa/15-April-2015-Visa-Rules-Public.pdf (last viewed Oct. 10, 2015) (describing Visa's "Merchant Chargeback Monitoring Program").

[239] *See, supra*, Section III.C.2; *see also* PX 13; PX 14.

[240] *See, supra*, Section III.C.3.

[241] *See, e.g.*, PX 14, pp. 25-26.

[242] *See, supra*, Section III.C.4.

C. The Scope of the Proposed *Ex Parte* Temporary Restraining Order is Appropriate in Light of Defendants' Conduct.

The overwhelming evidence demonstrates that the FTC will ultimately succeed in proving Defendants' law violations and that the balance of equities strongly favors upholding the public interest in addressing such violations. Preliminary injunctive relief is thus warranted. The FTC requests injunctive relief of three general types. As explained below, each type of ancillary relief is necessary to protect consumers and preserve the Court's ability to grant effective final relief.

1. The Court should enjoin Defendants from continuing to violate the law.

First, the FTC seeks to enjoin Defendants' ongoing law violations. The Proposed TRO includes provisions enjoining Defendants from continuing their scam and deceptive business practices.[243] Additionally, because Defendants rely on their business telephones and websites to lure consumers into their scheme, the TRO also includes provisions directing telephone providers and web hosting companies to disconnect or suspend the Corporate Defendants' phone numbers and websites.[244] Such TRO provisions have been ordered *ex parte* in appropriate FTC cases,[245] including cases involving "tech support scams," such as this one.[246]

---

[243] Proposed TRO, Section I (prohibits misrepresenting that they (1) are part of or affiliated with any company and (2) have detected security or performance issues in consumers' computers); Section II (prohibits using any false or misleading statement to induce any person to pay for any goods or services and violating the TSR); Section III (prohibits charging consumers for technical support services); Section IV (prohibits benefitting from or otherwise using consumers' information).

[244] Proposed TRO, Sections V-VI.

[245] *See, e.g.*, *FTC v. Navestad*, No. 09-6329 (W.D.N.Y. June 25, 2009) (granting *ex parte* TRO which, in part, enjoined defendants from violating the FTC Act and suspended Defendant's websites); *FTC v. Edge Solution, Inc.* No. 07-4087 (E.D.N.Y. Oct 12, 2007) (granting TRO which, in part, enjoined defendants from violating the FTC Act and suspended Defendants' websites); *FTC v. Career Hotline*, No. 09-1483 (M.D. FL. Sept. 8, 2009)) (ordered disconnection of defendants' phone numbers).

[246] *See, e.g., Boost Software*, No. 14-81397-CIV-MARRA (ordered conduct prohibitions and suspended websites); *Inbound Call Experts*, No. 14-81395-CIV-MARRA (ordered conduct

2. The Court should freeze Defendants' assets and order their transfer to the United States to preserve the possibility of providing restitution to Defendants' victims.

Second, the FTC seeks preliminary relief designed to help ensure the possibility of providing restitution to the victims of Defendants' scam. As explained above, and in the Certification of Plaintiff FTC Counsel Pursuant to Federal Rule of Civil Procedure 65(b) in Support of *Ex Parte* Motion for a Temporary Restraining Order and *Ex Parte* Motion to Seal Entire File ("Rule 65(b) Certification of Plaintiff FTC Counsel"), Defendants' unlawful business practices and deliberate attempts to conceal their identity lead the FTC to believe that Defendants will dissipate or conceal their assets once they learn of this action. Further, Defendants' have a demonstrated history of transferring at least part of their ill-gotten gains overseas.[247] Indeed, during 2013 and part of 2014 alone, Defendants transferred over $4.6 million to financial institutions in India.[248] This accounts for more than 25% of the approximately $17.9 million that Defendants took from consumers during that period.

The Proposed TRO includes provisions that would freeze Defendants' assets[249] and would require them to provide a financial accounting[250] so that the court-appointed receiver and the FTC may better identify and locate their assets. Additionally, the Proposed TRO includes provisions requiring Defendants to repatriate foreign assets[251] and preventing them from taking

---

prohibitions and suspended telephones and websites); *Pairsys*, No. 1:14-CV-1192 (same); *PCCare247*, No. 1:12-cv-07189-PAE (same).

[247] *See, supra*, Section III.F.

[248] *Id.*

[249] Proposed TRO, Section VII. The Proposed TRO would also allow the FTC to request from third parties or directly access any Defendant's consumer credit report. Proposed TRO, Section XII. This allows the FTC to identify third parties who might be holding Defendants' assets and should thus receive notice of the asset freeze order.

[250] Proposed TRO, Section VIII. The Proposed TRO would also require third parties holding Defendants' assets to retain and provide upon request records relating to those assets. Proposed TRO, Section IX.

[251] Proposed TRO, Section X.

steps that would preclude the repatriation of those assets.[252] Moreover, the Proposed TRO includes several provisions governing the duties and authority of a court-appointed temporary receiver,[253] who will aid in marshaling Defendants' assets, among other things. These types of TRO provisions have been ordered *ex parte* in appropriate FTC cases in the past.[254]

3. The Court should order the preservation and production of Defendants' business records and allow for an immediate access of Defendants' business premises in the United States.

Third, the FTC seeks preliminary relief designed to provide access to Defendants' records before those records can be destroyed. As detailed above, Defendants have gone to great lengths to conceal their identity.[255] Moreover, as explained more fully in the Rule 65(b) Certification of Plaintiff FTC Counsel, it is likely that Defendants will take steps to destroy documents that relate to their scam once they are notified of this action. The proposed order includes several provisions designed to grant access to Defendants' documents before they can be destroyed, including allowing immediate access to Defendants' business premises[256] and requiring Defendants to preserve records of their business activities.[257] Among other things, these records could potentially help the FTC uncover the extent of consumer harm inflicted

[252] Proposed TRO, Section XI.

[253] Proposed TRO, Sections XIV-XXIII.

[254] *See, e.g., Boost Software*, No. 14-81397-CIV-MARRA (freezing assets, allowing access to credit reports, appointing receiver); *Inbound Call Experts*, No. 14-81395-CIV-MARRA (same); *Pairsys*, No. 1:14-CV-1192 (freezing assets, requiring financial accounting and repatriation of assets, allowing access to credit reports, and appointing receiver); *PCCare247*, No. 1:12-cv-07189-PAE (freezing assets, requiring financial accounting and repatriation of assets, and allowing access to credit reports); *FTC v. CHK Trading Corp.*, No. 04-8686 (S.D.N.Y. Nov. 10, 2004) (requiring financial reporting); *FTC v. Epixtar Corp.*, No. 03-8511 (S.D.N.Y. Oct. 29, 2003) (freezing assets and requiring financial reporting); *FTC v. Five Star Auto*, No. 99-1693 (Mar. 8, 1999) (freezing assets, requiring financial statements, and repatriating foreign assets).

[255] *See, supra*, Section III.E.

[256] Proposed TRO, Section XVI.

[257] Proposed TRO, Section XIII.

by Defendants. These types of TRO provisions have been ordered *ex parte* in appropriate FTC cases in the past.[258]

4. The Court should issue the Proposed TRO *ex parte*.

An *ex parte* TRO is necessary because, if given notice, Defendants are likely to dissipate and conceal their assets and destroy evidence.[259] Defendants' fraudulent scheme,[260] deliberate concealment of their identity,[261] and history of shielding their ill-gotten gains[262] underscore the high likelihood that they will dissipate and hide assets and destroy evidence upon receiving notice of these proceedings. Indeed, providing premature notice of the Proposed TRO to Defendants would likely defeat the purpose of the TRO. This Court and others in the Third Circuit and throughout the nation have issued the type of preliminary relief the FTC seeks. To protect consumers, the FTC urges this Court to do so again in this matter.

V. CONCLUSION

Defendants operate a pernicious "tech support scam." They lure and deceive consumers in order to sell unnecessary services and take consumers' money. They have operated with

---

[258] *See, e.g., Boost Software*, No. 14-81397-CIV-MARRA (ordering immediate access and preservation of records); *Inbound Call Experts*, No. 14-81395-CIV-MARRA (same); *Pairsys*, No. 1:14-CV-1192 (ordering immediate access); *PCCare247*, No. 1:12-cv-07189-PAE (ordering preservation of records); *FTC v. Medical Billers Network, Inc.*, No. 05-2014 (S.D.N.Y. Feb. 18, 2005) (ordering preservation of records); *FTC v. Epixtar Corp.*, No. 03-8511 (S.D.N.Y. Oct. 29, 2003) (requiring defendants to retain records and granting immediate access); *FTC v. Five Star Auto*, No. 99-1693 (S.D.N.Y Mar. 8, 1999) (granting access to business records and preserving records).

[259] *See* Fed. R. Civ. P. 65(b)(1)(a) (authorizing *ex parte* relief when "immediate and irreparable injury, loss, or damage will result" upon notice); *In re Vuitton et Fils S.A.*, 606 F.2d 1, 5 (2d Cir. 1979) (permitting an *ex parte* TRO where notice would "only render fruitless further prosecution of the action"); *see also Vuitton v. White*, 945 F.2d 569, 575 (3d Cir. 1991) (district court should have granted an *ex parte* seizure order under the Trademark Counterfeiting Act of 1984 where "defendants were likely to destroy or hide the evidence if given notice of the proceedings").

[260] *See, supra*, Section III.A-B.

[261] *See, supra*, Section III.E.

[262] *See, supra*, Section III.F.

impunity for years and are continuing to exploit consumers. It is past time to put an end to Defendants' harmful lawlessness. For all the foregoing reasons, the FTC respectfully urges the Court to grant, *ex parte*, the Proposed TRO.

A Proposed TRO is attached.

Respectfully Submitted,

Dated: October 26, 2015

FIL M. DE BANATE, OH Bar # 86039
CHRISTOPHER D. PANEK, OH Bar # 80016
NICOLE J. GUINTO, OH Bar # 89319
Federal Trade Commission
1111 Superior Avenue East, Suite 200
Cleveland, Ohio 44114
Tel: (216) 263-3413 (de Banate)
Tel: (216) 263-3406 (Panek)
Tel: (216) 263-3435 (Guinto)
Fax: (216) 263-3426
fdebanate@ftc.gov
cpanek@ftc.gov
nguinto@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION