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

3. The balance of equities favors the

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.

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.

Defendant Bruce Bartolotta, also known as "Bruce Bart,"[24]

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

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.

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 s Tc-.t[(a…PX 52, Att4ch. A ("T.47 0 T11-.0001 Tc.0001 Tw(PX 3[(hey…s[H]e foremyna)4.

One consumer recalled becoming suspicious at first and told the telemarketer, "[M]aybe I

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.

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

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

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

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

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

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 .7[1.15 TD[(its D

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

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,

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

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

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

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 invol

C. The Scope of the Proposed Ex Parte

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]

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]