

RECEIVED

OCT - 3 2016

U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

GLOBAL ACCESS TECHNICAL SUPPORT LLC,
also d/b/a Global S Connect, Yubdata Tech, and
Technolive, a Missouri limited liability company;

GLOBAL SMIND LLC, also d/b/a Global S
Connect, a Missouri limited liability company;

SOURCE PUNDIT LLC, also d/b/a OneSource
Tech Support, a Missouri limited liability company;

HELIOS DIGITAL MEDIA LLC, a Missouri
limited liability company;

VGLOBAL ITES PRIVATE LIMITED, an Indian
corporation;

RAJIV CHHATWAL, individually and as an owner
or officer of Global Access Technical Support LLC,
Helios Digital Media LLC, and Source Pundit LLC;

RUPINDER KAUR, individually and as an owner
or officer of Global sMind LLC, and

NEERAJ DUBEY, individually and as an owner or
officer of Helios Digital Media LLC and VGlobal
ITES Private Limited.

Defendants.

Case No. _____

[FILED UNDER SEAL]

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

I. INTRODUCTION

The Federal Trade Commission asks this Court to halt a fraudulent operation that deceives consumers into purchasing worthless technical support services by leading them to believe that their computers have been infected by malware, viruses, or are experiencing significant performance issues. Operating under various names, including Global Access Technical Support (“GATS”), Defendants use pop-up internet advertisements to trick consumers into calling their India-based telemarketing boiler room. The advertisements are designed to look like an alert generated from within the consumer’s operating system or from a recognized technology company such as Microsoft or Apple, warning that serious performance or security issues have been detected with the consumer’s computer. The advertisements urge consumers to call a toll-free number registered to Defendants for assistance. During calls with consumers, Defendants claim that they are affiliated with or certified by Microsoft and Apple to service computers running the Windows and OS X operating systems. After gaining remote access to consumers’ computers, Defendants purport to run a series of “diagnostic” tests and inevitably report to consumers that the tests have detected the existence of viruses, malware, hackers, serious performance issues, or other threats. Defendants assert that these problems pose serious risks to consumer’s computers, and should be repaired immediately. Finally, after both frightening consumers and earning their trust, Defendants persuade them to spend hundreds of dollars for dubious “repairs” and tech support contracts.

In truth, Defendants are not affiliated with or certified by Microsoft or Apple, nor at the time consumers see the pop-up do Defendants have any way of identifying problems with consumers’ computers. The subsequent transactions between Defendants and consumers are

predicated on these misrepresentations. Operating this deceptive scheme since at least 2013, Defendants have bilked consumers out of more than \$5 million.

Unfortunately, technical support scams like the one perpetrated by Defendants are on the rise. In 2015, for example, the FTC received nearly 40,000 complaints from consumers about this type of scam, a dramatic increase over the previous year.¹ In June 2016, moreover, the FBI's Internet Crime Complaint Center issued an alert regarding a recent spike in complaints about technical support scams, noting that it had received over 3600 complaints in the first four months of this year.² The FTC has responded to this alarming trend by taking action against a series of companies engaged in conduct virtually identical to that here.³ Despite these actions, operations like GATS have persisted with their deceptive schemes.

The FTC brings this motion *ex parte* to freeze Defendants' assets and bring an immediate halt to their ongoing unlawful conduct. In support of this motion, the FTC submits overwhelming evidence of each Defendant's participation in this scheme, and of the deceptive nature of the conduct, including sworn statements from several of Defendants' consumer victims, a computer security expert who analyzed two undercover transactions conducted by an FTC investigator, and representatives from Microsoft and Apple. The persistent deception and the international components of this operation, including the frequent transfer of funds to India,

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

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

³ See, e.g., *FTC v. Big Dog Solutions LLC, et al*, No. 16-cv-6607 (N.D. Ill. June 24, 2015); *FTC v. Click4Support, LLC*, No. 15-5777 (E.D. Pa. Oct. 10, 2015); *FTC v. Pairsys, Inc.*, No. 14-cv-1192 (N.D.N.Y. Sept. 30, 2014); *FTC v. Inbound Call Experts, LLC*, No. 14-81395-CIV-MARRA (S.D. Fla. Nov. 14, 2014); *FTC v. Boost Software, Inc.*, No. 14-81397-CIV-MARRA (S.D. Fla. Nov. 12, 2014); *FTC v. PCCare247 Inc.*, No. 1:12-cv-07189-PAE (S.D.N.Y. Sept. 25, 2012); *FTC v. Pecon Software Ltd.*, No. 12-cv-7186-PAE (S.D.N.Y. Sept. 25, 2012); *FTC v. Marczak*, No. 12-cv-7192-PAE (S.D.N.Y. Sept. 25, 2012); *FTC v. Finmaestros, LLC*, No. 12-cv-7195-PAE (S.D.N.Y. Sept. 25, 2012); *FTC v. Lakshmi Infosoul Servs. Pvt. Ltd.*, No. 12-cv-7191-PAE (S.D.N.Y. Sept. 25, 2012).

present a very real risk that Defendants would hide or dissipate assets if they received notice of this action. The requested relief, including an asset freeze and the appointment of a temporary receiver, is necessary to preserve the Court's ability to provide effective final relief to Defendants' thousands of victims.

II. DEFENDANTS' ILLEGAL BUSINESS PRACTICES

A. Defendants' Deceptive Online Marketing

Defendants utilize online pop-up ads to make initial contact with consumers. The pop-up ads appear suddenly on consumers' computers and warn that the computers are experiencing security vulnerabilities or other technical problems that require immediate attention.⁴ Defendants pay affiliate advertisers to place these advertisements.⁵ The sole aim of this "pay per call" model of advertising is to generate telephone calls to Defendants' telemarketing boiler room in India, so that Defendants can sell consumer technical support services. Defendants have misled thousands of consumers into making such phone calls.

Consumer victims report that Defendants' pop-ups reference Microsoft,⁶ Apple⁷ or other well-known technology companies such as Norton⁸ or Verizon.⁹ This leads consumers to believe that the pop-up is actually a warning or message coming from one of those trusted

⁴ See PX 8, Declaration of Madoka Bernal ("Bernal Dec.") ¶ 4; PX 9, Declaration of Oleta Dorsey ("Dorsey Dec.") ¶ 3; PX 10, Declaration of Jeff Glasscock ("Glasscock Dec.") ¶ 3; PX 11, Declaration of Dawn Huffey ("Huffey Dec.") ¶ 3; PX 12, Declaration of Dagmar Lorenz ("Lorenz Dec.") ¶ 3; PX 13, Declaration of Norma Maxvill ("Maxvill Dec.") ¶ 4; PX 14, Declaration of Charles Tickner ("Tickner Dec.") ¶ 4; PX 15, Declaration of Robert Weaver ("Weaver Dec.") ¶ 4.

⁵ PX 1, Declaration of FTC Investigator Joseph F. Einikis III ("Einikis Dec.") ¶¶ 151 - 157, Attachment ("Att.") MMM (Defendants paid \$1,251,789.36 for pay per call advertising from November 2014 through June 2016); PX 7, Declaration of Bill Smith ("Smith Dec.") ¶ 24, Att. F at p. 2 ("GATS uses a PPC (pay per call) model of advertising on the internet").

⁶ See PX 7, Smith Dec. ¶ 38 (summarizing consumer complaints); PX 8, Bernal Dec. ¶ 4; PX 11, Huffey Dec. ¶ 3; PX 12, Lorenz Dec. ¶ 3; PX 13, Maxvill Dec. ¶ 4.

⁷ PX 1, Einikis Dec., ¶ 115.a. (consumer complained in chargeback that GATS claimed to be "Apple Care").

⁸ PX 14, Tickner Dec. ¶ 4.

⁹ PX 15, Weaver Dec. ¶ 4.

sources. Some consumers also describe a “persistent” or “incessant” alarm¹⁰ or a “terrible, loud sound along with a voice recording”¹¹ that accompanies Defendants’ pop-ups. Often, once the pop-up appears, consumers are unable to navigate away from the advertisement, rendering their computers unusable.¹² Sometimes the pop-up persists even after a consumer restarts his computer.¹³

Defendants’ pop-ups cause consumers to panic and fear that they will lose data from their computers or that their personal information has been exposed to hackers. This creates an urgency for consumers to remedy the perceived problems with their computers.¹⁴ The advertisements list a telephone number to call for immediate assistance, and consumer victims often feel that they have no choice but to call in order to regain control of their computers and fix any security or performance issues.

Creating the impression that the pop-up is generated from within the consumer’s computer is a key component of Defendants’ deceptive practices. In a blog post on its website, F5 Media, an affiliate advertising company to which Defendants have paid nearly \$1 million, encourages pop-up designs that look “undeniably realistic” or that give the consumer the impression that “Firefox, or Explorer notice something is wrong” with the computer.¹⁵ In the same blog post, F5 leads its clients to Google image search results for the phrase “windows virus

¹⁰ PX 8, Bernal Dec. ¶ 4 (“a loud and persistent beeping alarm”); PX 15, Weaver Dec. ¶ 4 (“loud, persistent beeping alarm”).

¹¹ PX 12, Lorenz Dec. ¶ 3 (“my computer also began to play a terrible, loud sound along with a voice recording indicating that my computer had been severely compromised”).

¹² See PX 8, Bernal Dec. ¶ 4; PX 9, Dorsey Dec. ¶ 3; PX 10, Glasscock Dec. ¶ 4; PX 11, Huffey Dec. ¶ 3; PX 12, Lorenz Dec. ¶ 3; PX 13, Maxvill Dec. ¶ 4; PX 14, Tickner Dec. ¶ 4; PX 15, Weaver Dec. ¶¶ 4 and 5; PX 7, Smith Dec. ¶ 38 (summarizing consumer complaints).

¹³ PX 8, Bernal Dec. ¶ 4 (even after restarting, “each time I opened the internet browser, the pop-up ad instantly reappeared, along with the beeping alarm”).

¹⁴ PX 8, Bernal Dec. ¶ 4; PX 9, Dorsey Dec. ¶ 4; PX 11, Huffey Dec. ¶ 4; PX 12, Lorenz Dec. ¶ 4; PX 15, Weaver Dec. ¶ 5.

¹⁵ PX 1, Einikis Dec. ¶ 154, Att. LLL (capture of F5 Media website).

popup” to show a “treasure trove of ideas” for these ad campaigns.¹⁶ There is no question that Defendants’ pop-ups are of no actual technical value, and are nothing more than an advertisement used to lure consumers into contacting Defendants’ call center.¹⁷

B. The Sales Call

Over time, Defendants’ pop-ups have displayed various toll-free numbers that are registered to Defendants.¹⁸ The pop-ups urge consumers to call these numbers for technical support.¹⁹ Once connected to the Defendants’ telemarketers, Defendants continue to mislead consumers into believing that they are dealing with Microsoft- or Apple-certified technical support personnel. Relying on this false marker of legitimacy to gain consumers’ trust, the telemarketers insist on remotely accessing consumers’ computers to perform a series of “diagnostic” tests. Defendants invariably tell consumers that the “diagnostic” has identified significant problems with their computers, and convince consumers to pay hundreds of dollars for unnecessary “repairs” and service.²⁰

1. Defendants Mischaracterize Their Pop-Ups

Defendants’ telemarketers use the presence of the pop-up to convince consumers that there are serious problems with their computers. For example, in an undercover recorded

¹⁶ *Id.*

¹⁷ Microsoft has provided a declaration stating unequivocally that its Windows computer operating systems do not include a feature designed to notify users of suspected performance or security problems through the use of pop-up messages. *See* PX 3, Declaration of Shawn Aebi, Service Delivery Manager for Consumer Services, Customer Service and Support, Microsoft Corporation (“Aebi Dec.”) ¶ 5.

¹⁸ *See* PX 1, Einikis Dec. ¶ 31, Att. N (records from phone provider Vonage showing toll-free numbers registered to Defendants).

¹⁹ *See* PX 8, Bernal Dec. ¶ 4; PX 9, Dorsey Dec. ¶ 4; PX 10, Glasscock Dec. ¶¶ 3-4; PX 11, Huffey Dec. ¶ 3; PX 12, Lorenz Dec. ¶ 3; PX 13, Maxvill Dec. ¶ 4; PX 14, Tickner Dec. ¶ 4; PX 15, Weaver Dec. ¶¶ 4 and 5; PX 7, Smith Dec. ¶ 38 (summarizing consumer complaints).

²⁰ *See* PX 8, Bernal Dec. ¶¶ 5-6 (\$300); PX 9, Dorsey Dec. ¶¶ 6-7 (\$269.95); PX 10, Glasscock Dec. ¶¶ 7-9 (\$299.75); PX 11, Huffey Dec. ¶¶ 7-8 (\$199.99); PX 12, Lorenz Dec. ¶¶ 6-7 (\$239.50, charge ultimately reversed); PX 13, Maxvill Dec. ¶¶ 6-8 (\$299.99); PX 14, Tickner Dec. ¶ 6 (GATS telemarketer gave price of \$599, but consumer refused to pay); PX 15, Weaver Dec. ¶¶ 7-10 (\$299.99); PX 7, Smith Dec. ¶ 39 (summarizing consumer complaints).

telephone call with an FTC investigator, one of Defendants' telemarketers insisted that the pop-up would only have appeared on the investigator's computer if it was experiencing problems. The telemarketer told the FTC investigator that he was "very very sure that the computer was having viruses" based only on the investigator's statement that the pop-up had appeared on the computer.²¹ In fact, the pop-up had not appeared, and the computer was newly formatted and free of any operational or security problems.²² Of course, at the time any consumer encounters Defendants' pop-up, Defendants have no information about the operating or security status of that consumer's computer.

2. Defendants' False Claims of Affiliation or Certification

Defendants' telemarketers then also perpetuate the ruse that Defendants are affiliated with well-known U.S. technology companies, or certified by Microsoft and Apple to provide technical support for those companies' products.²³ Having encountered the Defendants' pop-ups, which make the initial affiliation claims, consumers often ask Defendants' telemarketers directly if they are speaking with Microsoft technical support, wanting confirmation that they are dealing with a legitimate and trustworthy company. The telemarketers assure consumers that they are "official Microsoft" representatives²⁴ or "Microsoft certified technicians."²⁵ In an undercover call with an FTC investigator, Defendants' telemarketers assured him that "we all are

²¹ PX 1, Einikis Dec. ¶ 53, Att. X (transcript of first undercover purchase).

²² PX 2, Declaration of Jeffrey McJunkin, Expert ("McJunkin Dec.") ¶ 13 ("In my expert opinion, the initial state of the computer system for each of the calls contained no security or performance problems.").

²³ See PX 8, Bernal Dec. ¶ 5; PX 10, Glasscock Dec. ¶ 5; PX 11, Huffey Dec. ¶ 5; PX 12, Lorenz Dec. ¶¶ 4, 6, and 10 (consumer repeatedly asked if GATS telemarketers were "official Microsoft representative[s]," and telemarketers indicated they were); PX 13, Maxvill Dec. ¶¶ 7-8, Att. A (GATS telemarketer provided document indicating he was "online microsoft certified"); PX 14, Tickner Dec. ¶ 6 (GATS telemarketer claimed affiliation with Symantec); PX 15, Weaver Dec. ¶ 6 (GATS telemarketer claimed affiliation with Verizon); PX 7, Smith Dec. ¶ 38 (summarizing consumer complaints). See also PX 1, Einikis Dec. ¶¶ 54, 75, and 114 Atts. X and CC (GATS telemarketers claim Microsoft and Apple affiliations in undercover purchases, including complaint to Royal Canadian Mounted Police).

²⁴ PX 12, Lorenz Dec. ¶¶ 4, 6, and 10.

²⁵ PX 8, Bernal Dec. ¶ 5; PX 13, Maxvill Dec. ¶¶ 7-8, Att. A.

here Microsoft certified technician in Microsoft product and also Apple Mac computer as well, okay.”²⁶ A nearly identical statement was made in a second undercover call.²⁷

These claims of affiliation and certification are crucial components of Defendants’ scheme. They also are false. Defendants are not affiliated with Microsoft or Apple, nor are they certified to provide technical support services for their products.²⁸

3. Defendants’ Fraudulent “Diagnostic Tests”

Having gained consumers’ trust by falsely claiming to be affiliated with or certified by Microsoft or Apple, Defendants’ telemarketers request remote access to consumers’ computers so that they may perform a “diagnostic” scan and analysis.²⁹ Remote access gives telemarketers control over the computers, enabling them to move cursors, enter commands, run applications, and access stored information.³⁰ Once telemarketers have control over consumers’ computers, they begin a series of steps, which they describe as “diagnostic tests.” These are very similar to the “diagnostics” performed by defendants named in FTC enforcement actions against other tech support scams.³¹ Specifically, GATS telemarketers misrepresent the meaning of information displayed in applications built into the Windows operating system to “diagnose” problems with consumers’ computers. In reality, these are not actual tests, but are instead part of Defendants’

²⁶ PX 1, Einikis Dec. ¶ 54, Att. X.

²⁷ *Id.* at ¶ 75, Att. CC.

²⁸ See PX 3, Aebi Dec. ¶ 4; PX 4, Declaration of Julie Crawford (“Crawford Dec.”) ¶ 5.

²⁹ See PX 8, Bernal Dec. ¶¶ 5-6; PX 9, Dorsey Dec. ¶¶ 6-7; PX 10, Glasscock Dec. ¶¶ 7-9; PX 11, Huffey Dec. ¶¶ 7-8; PX 12, Lorenz Dec. ¶¶ 6-7; PX 13, Maxvill Dec. ¶¶ 6-8; PX 14, Tickner Dec. ¶ 6; PX 15, Weaver Dec. ¶¶ 7-10; PX 7, Smith Dec. ¶ 39 (summarizing consumer complaints).

³⁰ Defendants remotely access consumer’s computers using a service provided by LogMeIn. See PX 1, Einikis Dec. ¶¶ 56 and 63; PX 14, Tickner Dec. ¶ 6.

³¹ See, e.g., *FTC v. Big Dog Solutions LLC, et al*, No. 16-cv-6607 (N.D. Ill. June 24, 2015); *FTC v. Click4Support, LLC*, No. 15-5777 (E.D. Pa. Oct. 10, 2015); *FTC v. Pairsys, Inc.*, No. 14-cv-1192 (N.D.N.Y. Sept. 30, 2014); *FTC v. Inbound Call Experts, LLC*, No. 14-81395-CIV-MARRA (S.D. Fla. Nov. 14, 2014).

sales pitch, designed to confuse consumers and convince them that their computers are in need of service.

Defendants' fraudulent diagnostic is demonstrated in an undercover purchase conducted by the FTC. For this purchase, the FTC used a computer running a clean version of the Windows operating system, free of any malicious programs or other threats.³² Nevertheless, the GATS telemarketer claimed to discover evidence of significant problems with the computer. For instance, the GATS telemarketer, who identified himself as "Johnny," claimed that there were "junk files in your computer right now, which needs to be removed from your computer which makes your computer very, very slow. It is also possible that you have some viruses in between these folders."³³ Johnny also claimed that "stopped" services shown on the Microsoft System Configuration Utility ("msconfig") tab meant that the computer was not in "running condition."³⁴ Johnny then accessed the computer's "Event Viewer" and indicated that any "warnings" shown there meant parts of the computer were operating in an "error state," indicating a "problem with the boot up."³⁵ When the investigator asked if there were viruses on his computer, Johnny said, "Yeah, there are a lot of viruses in your computer."³⁶

After identifying these purported problems with the FTC's computer, Johnny told the FTC investigator that he could only fix them if the investigator purchased services from GATS.³⁷ He also warned that if the investigator were to try to fix some of the problems on his own, he

³² PX 2, McJunkin Dec. ¶ 13 ("In my expert opinion, the initial state of the computer system for each of the calls contained no security or performance problems.").

³³ PX 1, Einikis Dec. ¶ 53, Att. X (transcript of first undercover purchase).

³⁴ PX 1, Einikis Dec. ¶ 58, Att. X and Y (transcript and screen shot from first undercover purchase).

³⁵ PX 1, Einikis Dec. ¶ 59, Att. X and Z (transcript and screen shot from first undercover purchase).

³⁶ PX 1, Einikis Dec. ¶ 63, Att. X (transcript from first undercover purchase).

³⁷ *Id.*

risked problems booting up or losing internet connectivity with his computer.³⁸ Consistent with consumers' experiences with GATS, Johnny offered a one-time fix of these purported problems for \$150 or a year-long service contract for \$250.³⁹

Jeffrey McJunkin, a computer forensics and security expert retained by the FTC, has analyzed the hard drives and memory captures associated with the computers used in each of the FTC's undercover calls.⁴⁰ Mr. McJunkin has concluded that the FTC's computers prior to each undercover call were in a "clean state," had no "malware or infections," and contained no security or performance problems.⁴¹ Moreover, Mr. McJunkin found that the telemarketers in both calls made misleading statements about their "diagnoses" and "repairs" of the FTC's computers.⁴²

For example, Mr. McJunkin concludes that the telemarketer had "absolutely no data to back up the statement that 'you have some viruses in between these folders.'"⁴³ Mr. McJunkin further notes that contrary to the GATS telemarketer's statements, it is perfectly normal for a computer to have many "stopped" services and a whole host of startup programs.⁴⁴ Also false is the telemarketer's representation that the investigator risked losing Internet connectivity or problems booting up his computer if he attempted to delete startup programs on his own, rather than paying for specialized technical support.⁴⁵

³⁸ PX 1, Einikis Dec. ¶ 58, Att. X (transcript from first undercover purchase).

³⁹ PX 1, Einikis Dec. ¶ 62, Att. X (transcript from first undercover purchase). Interestingly, when the FTC investigator insisted on paying for the services with a credit card rather than by e-check, Johnny imposed a \$40 surcharge. See PX 1, Einikis Dec. ¶¶ 64-65. A similar surcharge was applied for the same reason in the FTC's second undercover call. *Id.* at ¶ 74.

⁴⁰ PX 2, McJunkin Dec. ¶¶ 5-8.

⁴¹ *Id.* ¶¶ 11-13.

⁴² *Id.* ¶¶ 24-50.

⁴³ *Id.* ¶¶ 28-30.

⁴⁴ *Id.* ¶¶ 33-35.

⁴⁵ *Id.* ¶¶ 39-40. Mr. McJunkin also concludes that the GATS representative made misrepresentations in the FTC's second undercover call, including telling the investigator that in providing "repair" services, "we took out the viruses as well." Of course, the computer was free from

4. The Sale

Having deceived consumers into believing that there are critical security or operating problems with their computers, Defendants offer consumers two options: a one-time fix to address the identified problems or a year-long service contract. The prices offered to consumers vary from \$150 for the one-time fix to \$500 or more for the year-long contract.⁴⁶ Defendants will increase the price if the service is for more than one computer. One consumer hesitated to purchase technical support from GATS, and the GATS telemarketer then reinstated the pop-up onto her computer.⁴⁷ The consumer ultimately agreed to pay, in order to have the pop-up removed.⁴⁸

GATS has collected payments from consumers by check, electronic check, and credit card.⁴⁹ Defendants' credit card processing accounts have consistently experienced high levels of chargeback requests from consumers, with many consumers insisting that the charges to Defendants were a result of fraud or were otherwise unauthorized.⁵⁰ In an attempt to defeat chargeback requests, Defendants began using online contracting services such as HelloSign⁵¹ or DocuSign⁵² to acquire signatures from consumers, which they use to challenge chargebacks by attempting to show authorization for the charges. Despite these contracts, however, Defendants

viruses from the outset. In fact, the scan run by GATS, clearly "didn't find any evidence of adware, malware, or viruses." *Id.* ¶¶ 47-50.

⁴⁶

⁴⁷ PX 12, Lorenz Dec. ¶ 7.

⁴⁸ *Id.* at ¶ 8.

⁴⁹ PX 1, Einikis Dec. ¶ 141.

⁵⁰ PX 1, Einikis Dec. ¶¶ 104.b. (3.75% chargeback rate); 115.d. (reasons for chargeback requests); 119, Att. TT (account reviewed due to high percentage of chargebacks totaling more than \$100,000); 131, Att. CCC (account exhibiting chargeback rate over 1% in first three months); 138 (chargeback rate of 2.88%). Defendants also returned over 7% of transactions by volume to consumers. PX 1, Einikis Dec. ¶¶ 139-140, Att. GGG.

⁵¹ PX 1, Einikis Dec. ¶ 30 and Att. XX p. 4

⁵² PX 12, Lorenz Dec. ¶ 8, Att. A.

still lost several credit card processing accounts due to excessive chargebacks.⁵³ As evidenced by the FTC's undercover purchases, Defendants are now pressuring consumers to pay by electronic check, presumably to limit the transactions being processed through credit card merchant accounts.⁵⁴ Moreover, some of the credit card processing accounts Defendants currently use were opened by third parties, not by Defendants themselves,⁵⁵ suggesting that banks may no longer be willing to take the risk of processing credit card charges for Defendants.

C. Consumer Injury

Defendants' illegal conduct has caused over five million dollars in consumer harm.⁵⁶ This harm, along with the scale of Defendants' operation, is reflected in records obtained from one of its telephone service providers, which show that from May 2014 to May 2016, Defendants' boiler room received calls from over 12,000 unique phone numbers, amounting to over 3700 hours of telephone sales calls.⁵⁷ Bank records also show that Defendants paid more than \$1.2 million to affiliate advertising companies that used the deceptive pop-ups to generate calls to Defendants' boiler room.⁵⁸

⁵³ PX 1, Einikis Dec. ¶ 107.a. (account terminated due to excessive chargebacks); ¶ 114.a. (same); ¶ 117, Att. RR (account terminated ; 4.45% chargebacks, "merchant account was detected for as a warning, the account had refunds and disputes around almost 10% The merchant is operating an unqualified business model."); 119, Att. TT (account terminated).

⁵⁴ PX 1, Einikis Dec. ¶¶ 65 and 74, Atts. X and CC (transcripts of undercover calls showing surcharges of \$40 or more for use of credit cards).

⁵⁵ The two FTC undercover purchases were charged to a merchant account owned by Yubdatatech, which GATS telemarketers described as a "partner company" or "payment gateway" to GATS. The Yubdatatech website is registered to a Pennsylvania company. PX 1, Einikis Dec. ¶¶ 44, 68, 74, 79, and 82-85, Atts. X (transcript), CC (transcript), DD (confirmation emails), EE (credit card statements).

⁵⁶ PX 1, Einikis Dec. ¶ 147, Att. III (Analysis shows \$5,150,506.56 in revenue from January 2014 through June 2016).

⁵⁷ PX 1, Einikis Dec. ¶ 32.

⁵⁸ PX 1, Einikis Dec. ¶ 157, Att. MMM (\$1,251,789.36 paid for pay-per-call advertising).

II. DEFENDANTS

Defendants are five corporations and the three individuals who own, direct, and manage this scheme as well as share in its profits. They are located in Missouri and India. As described below, the five corporations operate as a common enterprise.

A. Missouri Defendants

The hub of Defendants' domestic operations is St. Louis, Missouri. **Rajiv Chhatwal**, a St. Louis resident, incorporated Defendant **Global Access Technical Support LLC** and is the registered agent for **Source Pundit LLC**, two Missouri corporations through which this scheme operates.⁵⁹ Source Pundit and GATS are both registered to Chhatwal's residence in St. Louis.⁶⁰ Through these two companies, Chhatwal has acquired bank accounts,⁶¹ merchant processing accounts⁶² and internet domains⁶³ that have been used to collect consumer payments and create an internet presence for GATS. Under Chhatwal's direction, both GATS and Source Pundit have made large payments to affiliate advertising companies in the U.S. and Canada, as well as large transfers to Indian call centers.⁶⁴

Chhatwal and Defendant **Rupinder Kaur**, who is the registered agent of Defendant **Global sMind LLC**,⁶⁵ also work together to further the scheme. Kaur and Chhatwal are both authorized signers on several Global sMind bank accounts,⁶⁶ and jointly applied for merchant

⁵⁹ PX 1, Einikis Dec. ¶¶ 7, 9, and 14 Atts. A and B (corporate records).

⁶⁰ *Id.*

⁶¹ PX 1, Einikis Dec. ¶¶ 88 (GATS bank account summary) and 93 (Source Pundit bank account summary), Att. GG (overall bank account summary).

⁶² PX 1, Einikis Dec. ¶¶ 101, 108, 118, 123, 127, 134, and 147 Atts. HH (Source Pundit merchant account application), MM (GATS merchant account application), SS (same), WW (same), ZZ (same), EEE (same), and III (summary revenue chart).

⁶³ PX 1, Einikis Dec. ¶¶ 34-35, Att. O (summary chart).

⁶⁴ PX 1, Einikis Dec. Atts. JJJ (summary of transfers to VGlobal call center) and MMM (summary chart of advertising payments).

⁶⁵ PX 1, Einikis Dec. ¶ 8, Att. B (corporate records).

⁶⁶ PX 1, Einikis Dec. Att. GG (bank account summary).

processing accounts that received payments from consumer victims.⁶⁷ Operating as Global sConnect, Chhatwal and Kaur have collected over \$800,000 from victims of tech support scams.⁶⁸

Defendant **Helios Digital Media LLC**, was recently created to further this scheme. In opening a bank account for Helios, Chhatwal identified himself as an owner of the company, although he kept his name off Helios's official corporate records.⁶⁹ The Helios bank records show significant deposits from other companies that are processing consumer payments for Defendants and significant payments out to affiliate advertisers and to Defendant VGlobal, which operates Defendants' call center.⁷⁰ The bank statements for Helios are sent to Chhatwal's home.⁷¹

B. India Defendants

Defendant **Neeraj Dubey**, who lives in India, is the Director of Defendant **VGlobal ITES Private Limited**, a company located in New Delhi.⁷² Defendants use VGlobal to operate the call center that receives consumer calls in response to the pop-up messages.⁷³ Since 2014, the U.S.-based corporate defendants have transferred over \$1 million to VGlobal.⁷⁴ Dubey also is a co-owner of Helios.⁷⁵ Dubey recently traveled to the United States for business meetings in

⁶⁷ PX 1, Einikis Dec. ¶¶ 116, 120, and 133, Atts. QQ (Global sMind merchant account application), UU (same), and DDD (same).

⁶⁸ PX 1, Einikis Dec. ¶ 143 (From October 2014 through June 2016, Global sMind received approximately \$851,579.08 net revenue from consumers.).

⁶⁹ PX 1, Einikis Dec. ¶¶ 10, 95-96, Att. D (corporate records).

⁷⁰ PX 1, ¶¶ 149, 157, Att. MMM (From April 2016 to June 2016, Helios transferred \$170,000 to VGlobal and \$347,000 to pay-per-click advertisers).

⁷¹ PX 1, Einikis Dec. ¶ 95.

⁷² PX 1, Einikis Dec. ¶ 16 and Att. F (Customs and Border Patrol notes from encounter with Dubey at Chicago O'Hare airport).

⁷³ PX 7, Smith Dec. ¶ 36, Att. F.

⁷⁴ PX 1, Einikis Dec. ¶¶ 148-150, Att. JJJ.

⁷⁵ PX 1, Einikis Dec. ¶ 96.

several U.S. cities, including meetings with Chhatwal.⁷⁶ While in St. Louis, Dubey stayed with Chhatwal – his “business partner and friend” – in Chhatwal’s home.⁷⁷

C. Corporate Defendants Operate as a Common Enterprise

The named corporate defendants operate as a common enterprise and are therefore jointly and severally liable for each other’s illegal conduct. *F.T.C. v. Think Achievement Corp.*, 144 F. Supp.2d 993, 1011 (N.D. Ind. 2000) (“Where one or more corporate entities operate in common enterprise, each may be held liable for the deceptive acts and practices of the others”). To determine if a common enterprise exists, courts consider various factors, including: (1) maintaining officers and employees in common; (2) operating under common control; (3) sharing of office space; (4) operating the business through a maze of interrelated companies; (5) comingling of funds; and (6) sharing of advertising and marketing. *F.T.C. v. J.K. Publ’ns, Inc.*, 99 F. Supp.2d 1176, 1202 (C.D. Cal. 2000). Corporate Defendants meet this test.

The five corporate defendants here constitute a common enterprise. They operate a common scheme through a maze of interrelated companies that are commonly controlled. They use the same pop-up advertisements, the same telephone numbers, and they commingle funds. Chhatwal and Dubey, self-described “business partners,” created all of the corporate defendants, and together with Kaur maintain control over the finances, marketing, and operations of all of the corporate defendants. The individual defendants have transferred over \$1.3 million from the domestic corporate defendants to VGlobel, which operates the boiler room that Chhatwal described to the BBB as a “GATS owned operation.” The domestic corporate defendants have

⁷⁶ PX 1, Einikis Dec. ¶ 16 and Att. F (Customs and Border Patrol notes from encounter with Dubey at Chicago O’Hare airport).

⁷⁷ *Id.* CBP agents also found in Dubey’s bag a complaint from the Montana Department of Justice that contained a consumer complaint about “computer fraud” by “Global Concepts 10756 Trenton Ave. St. Louis, MO.”

paid affiliate advertisers over \$1 million for the deceptive pop-up ads that cause consumers to call Defendants' call center. Chhatwal has paid for dozens of toll-free telephone numbers that connect consumers to the India boiler room, and which are associated with several of the corporate defendants' websites.

III. ARGUMENT

Defendants' practices violate Section 5(a) of the FTC Act, 15 U.S.C. § 45(a). To prevent any further injury to consumers, the FTC asks that the Court issue *ex parte* the proposed TRO. This order would enjoin Defendants' ongoing law violations and would provide for other equitable relief designed to preserve the Court's ability to provide restitution to victims at the conclusion of the case.

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

The FTC Act provides that "in proper cases the Commission may seek, and after proper proof, the court may issue, a permanent injunction." 15 U.S.C. § 53(b). Once the Commission invokes the federal court's equitable powers, the full breadth of the court's authority is available, including the power to grant such ancillary final relief as rescission of contracts and restitution. *FTC v. Sec. Rare Coin & Bullion Corp.*, 931 F.2d 1312, 1314-15 (8th Cir. 1991) (*citing* *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1026 (7th Cir. 1988); *FTC v. U.S. Oil & Gas Corp.*, 748 F.2d 1431-34 (11th Cir. 1984); *FTC v. H.N. Singer, Inc.*, 668 F.2d 1107, 1113 (9th Cir. 1982)).

By enabling the courts to use their full range of equitable powers, Congress gave them authority to grant preliminary relief, including a temporary restraining order, preliminary injunction, and asset freeze. *U.S. Oil & Gas*, 748 F.2d at 1434 ("Congress did not limit the court's powers under the final proviso of § 13(b) and as a result this Court's inherent equitable

powers may be employed to issue a preliminary injunction, including a freeze of assets, during the pendency of an action for permanent injunctive relief.”). *See, e.g., FTC v. Neiswonger*, Case No. 4:96-CV-2225-SNL (E.D. Mo. July 17, 2006) (*ex parte* TRO with appointment of receiver, asset freeze, and expedited discovery in contempt matter); *FTC v. Real Wealth, Inc.*, Case No. 10-0060-CV-W-FJG (W.D. Mo. Jan. 26, 2010) (temporary restraining order with asset freeze); *FTC v. Grant Search, Inc.*, Civil No. 02-4174-CV-C-NKL (W.D. Mo. Aug. 15, 2002) (temporary restraining order with asset freeze). This Court therefore can order the full range of equitable relief sought and can do so on an *ex parte* basis. *U.S. Oil & Gas*, 748 F.2d at 1432 (authorizing preliminary injunction and asset freeze); *see also* S. Rep. No. 103-130, at 15-16 (1993), *as reprinted in* 1994 U.S.C.C.A.N. 1776, 1790-91 (“Section 13 of the FTC Act authorizes the FTC to file suit to enjoin any violation of the FTC [Act]. The FTC can go into court *ex parte* to obtain an order freezing assets, and is also able to obtain consumer redress.”).

This Court has personal jurisdiction over all of the Defendants, and venue is proper here. Because even the India-based Defendants have contacts with the United States, the Court has personal jurisdiction over them under the FTC Act’s nationwide service of process provision, 15 U.S.C. § 53(b). Moreover, under the FTC Act’s venue provision, an action may be brought wherever a corporation “resides or transacts business.” 15 U.S.C. § 53(b). In addition, venue is proper over a corporation wherever it is subject to personal jurisdiction. *See FTC v. Bay Area Bus. Council, Inc.*, No. 02-c-5762, 2003 WL 21003711, at *2 (N.D. Ill. May 1, 2003).

B. FTC Meets the Standard for Issuance of a Temporary Restraining Order

Two factors determine whether temporary injunctive relief should issue under Section 13(b): (1) the likelihood of success on the merits; and (2) the balance of equities. *See* 15

U.S.C. §53(b); *see also* *FTC v. Univ. Health*, 938 F.2d 1206, 1217 (11th Cir. 1991); *FTC v. World Travel Vacation Brokers Inc.*, 861 F.2d 1020 at 1029 (7th Cir. 1988); *FTC v. Business Card Experts, Inc.*, No. 06-4671, 2007 WL 1266636, at *3 (D. Minn. Apr. 27, 2007) (*citing* *FTC v. World Wide Factors Ltd.*, 882 F.2d 344, 347 (9th Cir. 1989)). Irreparable injury need not be shown because its existence is presumed in a statutory enforcement action. *World Wide Factors*, 882 F.2d at 346 (“under § 53(b), irreparable harm is presumed and the Court need only consider the FTC’s likelihood of success and the balance of any conflicting equities.”); *Univ. Health*, 938 F.2d at 1218. As set forth below, both considerations militate in favor of the requested relief.

1. Plaintiffs are Likely to Succeed on the Merits

To demonstrate a likelihood of success on the merits, the FTC must show that it will likely prevail. The record abounds with evidence that Defendants violate Section 5 of the FTC Act.

Defendants regularly misrepresent to consumers that they have identified a host of security or performance problem with consumers’ computers and that they are affiliated with or certified by Microsoft and Apple. A representation or practice is deceptive under Section 5(a) of the FTC Act, 15 U.S.C. §45(a), if it is material and likely to mislead consumers, acting reasonably under the circumstances. *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1095 (9th Cir. 1994); *Kraft, Inc. v. FTC*, 970 F.2d 311, 314 (7th Cir. 1992), *cert. denied* 507 U.S. 909 (1993); *Real Wealth Inc.*, 2011 WL 1930401, at *2 (*citing* *FTC v. Cyberspace.com, LLC*, 453 F.3d 1196, 1199 (9th Cir. 2006)). A representation is material if it is one upon which a reasonably prudent person would rely in making a purchase decision. *Sec. Rare Coin*, 931 F.2d at 1316; *Real Wealth Inc.*, 2011 WL 1930401, at *2; *FTC v. Mallett*, 818 F. Supp. 2d 142, 148 (D.D.C. 2011); *FTC v. Transnet Wireless Corp.*, 506 F. Supp. 2d 1247 (S.D. Fla. 2007). The Commission need

not prove actual reliance to establish materiality. *Sec. Rare Coin*, 931 F.2d at 1316; *Real Wealth Inc.*, 2011 WL 1930401, at *2; *Transnet*, 506 F. Supp. 2d at 1266-67. Express and deliberate claims are presumed material. *FTC v. SlimAmerica*, 77 F. Supp. 2d 1263, 1272 (S.D. Fla. 1999); *FTC v. Wilcox*, 926 F. Supp. 1091, 1098 (S.D. Fla. 1995). False claims are inherently “likely to mislead.” *In re Thompson Med. Co.*, 104 F.T.C. 648, 788 (1984), *aff’d*, *Thompson Med. Co. v. FTC*, 791 F.2d 189 (D.C. Cir. 1986), *cert. denied*, 479 U.S. 1086 (1987).⁷⁸ In deciding whether particular statements are deceptive, courts must look to the “overall net impression” that the statements create. *See Kraft*, 970 F.2d at 322; *FTC v. Stefanchik*, 559 F.3d 924, 928 (9th Cir. 2009).

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

Both of these core representations are false and unquestionably material. Defendants make these misrepresentations for the specific purpose of causing consumers to believe that there is something wrong with their computers and that Defendants can be trusted to fix these problems. These misrepresentations lead consumers to call Defendants and allow their computers to be accessed, which, in turn, enables Defendants to run their phony “diagnostic” and scare consumers into paying hundreds of dollars for Defendants’ products and services. Absent

⁷⁸ The FTC need not prove that Defendants acted with intent to defraud or in bad faith. *See, e.g., World Travel Vacation Brokers*, 861 F.2d at 1029; *Removatron Int’l Corp. v. FTC*, 884 F.2d 1489, 1495 (1st Cir. 1989); *FTC v. Five-Star Auto Club*, 97 F. Supp. 2d 502, 526 (S.D.N.Y. 2000).

these false claims, a reasonable consumer would not do business with Defendants, as Defendants are not affiliated with Microsoft and Apple, or certified to service their products, and Defendants have no idea whether there actually is anything wrong with consumers' computers.

Defendants' misrepresentations are likely to mislead reasonable consumers that GATS is affiliated with Microsoft or Apple or certified to service their products. As detailed by the declarations and other evidence submitted by the Commission, consumers form this belief because Defendants, both in their pop-ups and the ensuing sales pitch, repeatedly invoke the names of these companies. They also falsely reassure consumers that GATS and its "technicians" have received specialized training and certifications from Microsoft and Apple.

Consumers also reasonably believe that their computers are in need of immediate repair. Defendants go to great lengths to ensure this. They disseminate advertisements designed to look like warnings from consumers' computers. They then gain remote access to computers and misrepresent the significance of innocuous messages, files, and information found on those computers. Given the extent and complexity of these ruses, as well as the number of consumers deceived by them, Defendants' claims are likely to mislead reasonable consumers.

2. The Balance of Equities Strongly Favors Injunctive Relief

Once the FTC has shown a likelihood of success on the merits, the Court must balance the equities, giving greater weight to the public interest than to any of Defendants' private concerns. *World Travel*, 861 F.2d at 1029. The public equities here are compelling, as the public has a strong interest in halting the deceptive scheme, and in preserving the assets necessary to provide effective final relief to victims. *See FTC v. Sabal*, 32 F. Supp. 2d 1004, 1009 (N.D. Ill. 1998). Defendants, by contrast, have no legitimate interest in continuing to deceive consumers and persisting with conduct that violates federal law. *See id.*; *FTC v. World*

Wide Factors, 882 F.2d at 347 (upholding district court finding of “no oppressive hardship to defendants in requiring them to comply with the FTC Act, refrain from fraudulent representation or preserve their assets from dissipation or concealment.”). An injunction is necessary to ensure that Defendants do not continue their scheme while the case is pending.

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

The individual defendants are responsible for the illegal activity of the corporations they control.⁷⁹ An individual may be held liable for injunctive and monetary relief under the FTC Act if the individual: (1) participated directly in or had authority to control the practices, and (2) had some knowledge of the practices. See *Bay Area Bus. Council*, 423 F.3d 627, 636 (7th Cir. 2005); *World Media Brokers*, 415 F.3d at 764; *Amy Travel Serv., Inc.*, 875 F.2d at 573. Authority to control may be evidenced by “active involvement in business affairs and the making of corporate policy, including assuming the duties of a corporate officer.” *Amy Travel*, 875 F.2d at 573. The FTC does not need to show intent to defraud. *Id.* The knowledge requirement is satisfied by a showing that the defendant (1) had actual knowledge of the deceptive acts or practices, (2) was recklessly indifferent to the truth or falsity of the representations, or (3) had an awareness of a high probability of fraud coupled with an intentional avoidance of the truth. See *World Media Brokers*, 415 F.3d at 764; *Bay Area Bus. Council*, 423 F.3d at 636; *Amy Travel*, 875 F.2d at 574.

Each individual defendant is an officer of one or more of the corporate defendants, giving rise to a presumption of control. Voluminous evidence submitted by Plaintiff shows the direct

⁷⁹ As noted above in Section II.C., *supra*, the five corporate defendants do not function as independent legal entities, but as an interrelated network to facilitate Defendants’ scam. They are therefore jointly and severally liable for Defendants’ conduct because they have operated as a common enterprise. See *Del. Watch v. FTC*, 332 F.2d 745, 746 (2nd Cir. 1964); accord *FTC v. J.K. Publ’ns., Inc.*, 99 F. Supp. 2d 1176, 1202 (C.D. Cal. 2000); *FTC v. Wash. Data Res.*, 856 F. Supp. 2d 1247, 1271 (M.D. Fla. 2012); *FTC v. Direct Benefits Group, LLC*, 6:11-cv-1186-Orl-28TBS, 2013 WL 3771322, at *18 (M.D. Fla. July 18, 2013).

involvement of these individuals in managing their call center, controlling the finances of the operation, disseminating misleading advertising, and obtaining services used to facilitate the GATS operation.

Chhatwal has for years been apprised of consumer complaints about the misleading pop-ups and sale pitches, and has seen the resulting high chargeback rates lead to the closure of several merchant processing accounts. In 2015, Chhatwal contacted the Better Business Bureau of Eastern Missouri and Southern Illinois (“BBB”) seeking accreditation for GATS.⁸⁰ BBB Investigator Bill Smith undertook a review of the BBB’s internal file on the company as well as materials submitted by Chhatwal, ultimately denying the application.⁸¹ Prompted by a series of consumer complaints reporting the same kind of deceptive conduct, the BBB asked Chhatwal to explain what GATS intended to do to correct these problems.⁸² Chhatwal never responded, but a month later again applied for accreditation.⁸³ The BBB denied the second application.⁸⁴

In November 2015, after receiving additional consumer complaints, Smith attempted to speak with Chhatwal in person by visiting the business location at 10756 Trenton Avenue in St. Louis County. Chhatwal was not there, but a person who claimed to share office space with him said he would ask Chhatwal to contact Smith. When Smith did not hear from him, he sent an email to Chhatwal.⁸⁵ In his response, Chhatwal acknowledged to Smith that GATS used pop-up ads to generate leads, and conceded that consumers who encounter the ads may not know how to

⁸⁰ PX 7, Smith Dec. ¶ 6.

⁸¹ PX 7, Smith Dec. ¶¶ 7-13 (Smith reviewed consumer complaints, spoke with Chhatwal, and felt the advertising used by GATS was “highly deceptive”).

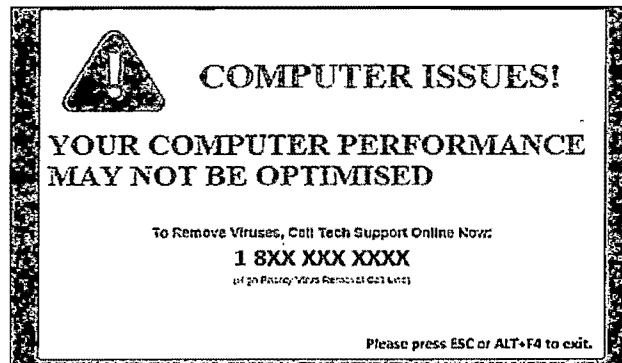
⁸² PX 7, Smith Dec. ¶ 14, Att. B (BBB “patterns letter” sent to GATS on July 23, 2015).

⁸³ PX 7, Smith Dec. ¶¶ 15-16.

⁸⁴ PX 7, Smith Dec. ¶ 17.

⁸⁵ PX 7, Smith Dec. ¶¶ 21-22. During this time, Smith also learned of the connection between Global sConnect and GATS from consumer complaints. *Id.* at ¶¶ 19-20. Smith conducted additional research on Global sConnect and determined that its website was then registered to Harinder Singh. He sent Singh an email, but the response came from Chhatwal. *Id.* at ¶¶ 30-32, Att. E.

close them out and feel locked in.⁸⁶ Chhatwal additionally provided written responses to questions posed by Smith, indicating that GATS “constantly monitor[s] the ads that are being published for content.”⁸⁷ Chhatwal provided the following sample advertisement, but it appears to be a heavily sanitized version of what GATS consumers have actually encountered.



Chhatwal’s central role in this scheme cannot be understated.

Dubey resides and works in New Delhi and directs the call center where the telemarketers actually make sales to consumers and where some consumers call to complain about the deceptive sales practices. Kaur is a 51% owner of Global sMind and has provided a personal guarantee on the Global sMind merchant processing accounts, alerting her to the high levels of chargeback requests from defrauded consumers.⁸⁸ Each of the individuals is a signer on business accounts that have paid hundreds of thousands of dollars to the affiliate advertising company that generates and places the deceptive pop-ups.

Given their control over and active participation in this scheme, the individual defendants are undoubtedly aware of the deceptive practices, and should therefore be subject to the injunction and the asset freeze.

⁸⁶ PX 7, Smith Dec. ¶ 24.

⁸⁷ PX 7, Smith Dec. ¶ 36 Att. F at p. 16.

⁸⁸ PX 1, Einikis Dec. ¶ 120, Att. UU.

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

An *ex parte* TRO is necessary and legally appropriate to prevent Defendants from dissipating assets and destroying evidence. The Commission respectfully requests a TRO to: (a) freeze Defendants' assets; (b) appoint a temporary receiver over the corporate defendants; and (c) grant the Commission immediate access to Defendants' records and information. Defendants are likely to dissipate assets or destroy evidence if given advance notice of the FTC's action.⁸⁹ District courts in the Eighth Circuit have frozen defendants' assets, appointed receivers, and granted the FTC immediate access to defendants' business premises in other FTC enforcement actions.⁹⁰ Similarly, other district courts have ordered such relief in FTC enforcement actions against remote tech support scams.⁹¹

1. Asset Freeze

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

⁸⁹ *See* Declaration and Certification of FTC Counsel Pursuant to Fed. R. Civ. P. 65(b) in Support of Plaintiffs' *Ex Parte* Motion for Temporary Restraining Order and Motion to Temporarily Seal File (describing need for *ex parte* relief and citing cases in which defendants who learned of impending FTC action withdrew funds, destroyed vital documents, and fled the jurisdiction).

⁹⁰ *See, e.g., FTC v. Business Card Experts, Inc.*, Case No. 0:06-CV-04671-PJS (D. Minn. Nov. 29, 2006) (*ex parte* TRO with appointment of receiver, asset freeze, and expedited discovery, including financial reporting); *FTC v. Kruchten*, Case No. 01-523-ADM/RLE (D. Minn. May 10, 2001) (*ex parte* TRO with appointment of receiver and asset freeze); *FTC v. Neiswonger*, Case No. 4:96-CV-2225-SNL (E.D. Mo. July 17, 2006) (*ex parte* TRO with appointment of receiver, asset freeze, and expedited discovery in contempt action); *FTC v. TG Morgan*, Case No. 4:91-CV-638-DEM (D. Minn. Aug. 26, 1991) (*ex parte* TRO with asset freeze, and immediate access to business premises); *FTC v. Sec. Rare Coin & Bullion Corp.*, Case No. 3:86-CV-1067 (D. Minn. Dec. 29, 1986) (granting FTC's *ex parte* TRO with asset freeze and financial accounting).

⁹¹ *See, e.g., See, e.g., FTC v. Big Dog Solutions LLC, et al*, No. 16-cv-6607 (N.D. Ill. June 24, 2015); *FTC v. Click4Support, LLC*, No. 15-5777 (E.D. Pa. Oct. 10, 2015); *FTC v. Pairsys, Inc.*, No. 14-cv-1192 (N.D.N.Y. Sept. 30, 2014); *FTC v. Inbound Call Experts, LLC*, No. 14-81395-CIV-MARRA (S.D. Fla. Nov. 14, 2014); *FTC v. Boost Software, Inc.*, No. 14-81397-CIV-MARRA (S.D. Fla. Nov. 12, 2014).

corporate defendants [are] available to make restitution to the injured consumers.” *Id.* at 1031.

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

2. Temporary Receiver

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

3. Immediate Access and Limited Expedited Discovery

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

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

To prevent Defendants from dissipating or concealing their assets, the requested TRO should be issued *ex parte*. An *ex parte* TRO is warranted when the facts show that immediate and irreparable injury, loss, or damage will occur before the defendants can be heard in opposition. *See* Fed. R. Civ. P. 65(b). Given the significant international components of this operation, and the large transfers of assets to India, there is a serious risk that assets and evidence stemming from Defendants' illegal activity will disappear if they receive prior notice. The blatantly deceptive nature of Defendants' scheme presents a serious risk that Defendants will destroy documents and dissipate assets if given advance notice of Plaintiffs' motion.⁹²

⁹² *See* Certification and Declaration of FTC Counsel pursuant to Rule 65(b).

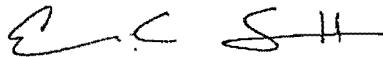
V. CONCLUSION

For the reasons set forth above, the Commission respectfully requests that the Court enter the proposed TRO to halt Defendants' violations of the FTC Act and to help ensure the possibility of effective final relief for consumers.⁹³

Dated: October 3, 2016

Respectfully submitted,

DAVID C. SHONKA
Acting General Counsel



Elizabeth C. Scott

Illinois Bar Number: 6278075
Samantha Gordon
Illinois Bar Number: 6272135
Federal Trade Commission, Midwest Region
55 West Monroe Street, Suite 1825
Chicago, Illinois 60603
escott@ftc.gov
sgordon@ftc.gov
(312) 960-5609 [Scott]
(312) 960-5623 [Gordon]

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

⁹³ Along with this Memorandum, Plaintiffs have submitted a proposed *Ex Parte* Temporary Restraining Order with Asset Freeze, Appointment of a Receiver, Other Equitable Relief and Order to Show Cause Why a Preliminary Injunction Should Not Issue.