No. 15-3937

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

FEDERAL TRADE COMMISSION, ET AL,
Appellee
v.

CLICK4SUPPORT, ET AL.,

SPANNING SOURCE, LLC; GEORGE SAAB;
CHETAN BHIKHUBHAI PATEL AND
NIRAJ PATEL,
Appellants,

On Appeal from the United States District Court
for the Eastern District of Pennsylvania,
No. 15-cv-5777
Hon. Stewart Dalzell

ADDENDUM TO BRIEF OF THE FEDERAL TRADE COMMISSION

DAVID C. SHONKA
Acting General Counsel

JOEL MARCUS
Director of Litigation

LESLIE RICE MELMAN
Assistant General Counsel

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
lmelman@ftc.gov

Of Counsel:
JON M. STEIGER
Director, East Central Region

FIL M. DE BANATE
CHRISTOPHER D. PANEK
Attorneys
FEDERAL TRADE COMMISSION
Cleveland, OH 44114

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

JURISDICTION

The district court had jurisdiction under Sections 5(a), 13(b), and 19 of the Federal Trade Commission Act (FTC Act), 15 U.S.C. §§ 45(a), 53(b), and 57b; and under 28 U.S.C. §§ 1331, 1337(a), and 1345. The district court entered an order for a preliminary injunction on November 10, 2015. A5. The court amended its order on November 25, 2015. A37. Appellants filed a timely notice of appeal from both the original and the amended orders on December 8, 2016. A1. This Court has jurisdiction under 28 U.S.C. § 1292(a).

QUESTION PRESENTED

Appellants joined an unlawful scheme to trick consumers into purchasing unnecessary computer support services. Appellants' role was to provide credit card processing and other services that were essential to the scheme's success. In return for their contributions, appellants received up to 8.5% of net consumer sales. The FTC charged appellants (and others involved in the scheme) with violating the FTC Act and the FTC's Telemarketing Sales Rule. At the agency's request, the district court preliminarily enjoined appellants from (1) continuing

to operate the scheme and (2) dissipating corporate assets pending adjudication of the merits. The question presented is:

Whether the district court abused its discretion in issuing the preliminary injunction.

INTRODUCTION

This appeal involves a technical services support scheme, known as Click4Support, that exploited consumers' fears about vulnerabilities on their computers. From at least May 18, 2012 until the district court entered an ex parte temporary restraining order (TRO), appellants participated in a scheme to trick consumers into buying unnecessary computer tech support services. The scheme was the brainchild of a businessman in India – Abhishek Gagneja. He needed access to a merchant account that would enable him to collect consumers' credit card payments.

To gain that access, Gagneja proposed a business venture to appellants. Appellants agreed to open a merchant account that would allow Gagneja's telemarketing operation to collect credit card payments. For their part, in setting up an initial account, appellants received a share of net consumer sales – initially, 8.5 %. Within a few weeks of

joining forces, appellants had ample reason in the form of excessive chargebacks to suspect that they were participating in a fraudulent scheme. They responded, however, by continuing to process charges, opening new merchant accounts, and assuming an even larger role in the scheme by responding to complaints, processing refund requests, and providing post-sale technical support.

The FTC and its co-plaintiffs (the Commonwealth of Pennsylvania and the State of Connecticut) filed an action in the United States District Court for the Eastern District of Pennsylvania. In an 11-count complaint, they alleged that appellants and others had violated Section 5 of the FTC Act, 15 U.S.C. § 45(a), the Telemarketing Act, 15 U.S.C. § 6102(c), and state consumer protection statutes by, *inter alia*, making deceptive representations about their affiliations with major tech companies and misleading consumers about their need for services.

The court granted the FTC's motion for a preliminary injunction, finding ample evidence that the corporate defendants comprised a common enterprise that transacted business through an "interrelated maze" (A71) in which Gagneja's companies provided technical services and appellants, for their part, managed the merchant accounts,

responded to consumer complaints, and processed refunds. A70-71. The court found that the individual defendants owned or managed the companies (*id.*) and therefore were personally liable for more than $17 million in consumer loss.[1]

No appellant denies that defendants' Click4Support scheme was a scam from start to finish. They contend that they merely provided services in the ordinary course of business – *i.e.*, credit card processing – and therefore any liability rests with the telemarketers in India.

Ample evidence supports the district court's conclusion that appellants participated in a common enterprise and are therefore responsible for the resulting consumer harm. Their services were the lifeblood of a scheme that, after its launch, generated volumes of complaints and alerted appellants of the deception. They responded to these alerts by assuming an even larger role in the scheme. They are

[1] The FTC's initial estimate of $17.9 million underestimates actual losses by $11.7 million. The additional $11.7 million represents additional consumer payments to defendants that were processed through other merchant accounts. Furthermore, the district court's preliminary findings do not include sums that thousands of consumers needed to expend to restore their computers. *See e.g.,* A947 (computer restoration cost $80); A1017 (increased security cost $122); A1057-58 (virus removal cost $100); A1064-66 (consumer purchased new computer and router); A1086 (consumer hired computer technician to remove malware).

thus rightfully bound by a preliminary injunction restraining their conduct and freezing their corporate assets pending disposition of the merits.

In rendering its decision on the FTC's motion for preliminary relief, the district court applied the proper standard – namely, a likelihood of success on the merits and a weighing of the equities. Appellants' assertions of procedural error are unfounded. The district court's decision to grant a preliminary injunction should be affirmed.

COUNTERSTATEMENT OF THE CASE

A. The "Technical Support" Scam

Abhishek Gagneja (Gagneja), a businessman based in India, wanted to make money by offering U.S. customers "tech support" provided by his firms, Innovazion Research Private Ltd. (Innovazion-India) and its U.S. counterpart, Innovazion Inc. (Innovazion-U.S.). To do this, Gagneja joined forces with appellants. Their goal was to sell consumers tech support services that they did not need, and defendants achieved this by making consumers believe that their computers had viruses, spyware, malware, security breaches, or other vulnerabilities. For over three years, defendants carried these goals on the backs of consumers, netting millions of dollars in the process.

Defendants' scheme relied on consumers' use of internet search engines – *e.g.*, Google – to troubleshoot problems with their computers.[2] By design, these search results included ads that invited consumers to call a toll-free number or click on a link to another website, which listed

[2] *See* A939; A942; A949; A970-72; A978; A993, A996; A1001; A1004; A1010; A1017; A1028; A1064; A1072-73; A1075; A1084; A1103.

a phone number.[3] In other instances, defendants lured consumers into calling their telemarketers using bogus pop-up messages – some of which displayed the Apple logo – telling consumers their computers were infected with malware.[4]

Thinking they were calling a legitimate U.S. technology company,[5] consumers who dialed the toll-free number, either directly or in response to a pop-up message, were connected to telemarketers in India. In many instances, the telemarketers claimed an affiliation with well-known U.S. technology firms,[6] a ploy they used to convince

---

[3] *See* A735, A770 (undercover call); A963 (consumer declaration); A993 (same); A1012 (same); A1044 (same); A1081 (same); A1103 (same).

[4] *See* A963 (displayed Apple Safari logo); A1043 (same). Consumers could not delete the pop-ups from their screens until they made a call to the displayed toll-free number. Defendants also solicited sales by calling consumers directly. *See*, *e.g.*, Doc. 76 at 8 (Gagneja Decl.); A1065.

[5] *See* A963; A1034; A1043; A1057-58; A1081.

[6] *See, e.g.*, A935 ("technical support that deals with Microsoft"); A1015 ("a Microsoft agent"); A1057-58 ("a senior certified Microsoft technician"); A1072-73 ("Microsoft technicians representing Cox"); A1111 (claimed to be from Charter and Microsoft); A1004 ("Google Support"); A1041 (claimed to be from Apple); A947 (same); A970, 972 (same); A1081 (same); A939 ("Apple iPhone Support"); A964 ("licensed by and registered with Apple"); A996 ("authorized tech support for Apple"); A959-60 ("[W]e also handle Dell product."); A1001 ("[I] was told that yes they were affiliated with Dell."); *see also* A976 ("HP Support"); A978 ("technical support for Comcast"); A1019 ("an employee of Brother

reluctant consumers to give them remote access to their computers.[7] The telemarketers invariably told consumers they needed direct access even when the problems that consumers identified had nothing to do with their computers.[8]

After gaining access, the telemarketers purported to diagnose malware, a virus, or other vulnerability that supposedly could be

---

International Printer Company"); A1084 ("work with AT&T"); A1099 ("working with Best Buy").

[7] *See* A939 ("They were TOTALLY DECEPTIVE, leading me to believe they were working for Apple."); A947 ("I was sure [I] had apple [on the phone] and asked them if they were [A]pple and they said yes."); A976 ("They made me think they were HP support * * *. I FOOLISHLY agreed to allow the remote access."); A978 (granted access after they claimed they "do technical support for Comcast"); A996 ("I was verbally told that they were authorized tech support of [A]pple * * *. I foolishly let them remote onto my machine * * *."); A1004 ("Before I gave him permission [for access], I again asked him if he was with Google Support. He again claimed that he was."); A1010 ("[T]hey said the only way to fix it was to get into my computer, I agreed trusting it was Cannon."); A1015 ("[R]epresenting himself as a Microsoft agent * * * he convinced me to give him control of my computer * * *."); A1019-21 ("[T]hinking I was dealing with a reliable representative for Brother Corporation I did [allow access]."); A1030 ("I agreed (thinking he worked for Best Buy.)"); A1057-58 ("I was told by a 'senior certified Microsoft technician' * * * and agreed * * * to access my computer."); A1081-82 ("[B]elieving I was dealing with a representative of Apple, I let him [control my computer].").

[8] *See, e.g.*, A939 ("update" appeared on consumer's Apple iPhone); A1039 (lost Apple iPhone contacts); A976 (printer issue); A1010 (same); A1015 (same); A1017 (same); A1052 (same); A1077 ("[I] needed to have the password reset [on my router].").

remedied by purchasing their tech support services. *See, e.g.*, A1034; A1043; A1057-58. During remote access sessions, telemarketers controlled consumers' computers and were able to view the computer screen, control the mouse or cursor, enter commands, run applications, and access stored information. *See, e.g.,* A304, 307, 314. This enabled them to execute various commands that purportedly revealed the cause of consumers' technological problems. Once they accessed the computers, they used a variety of tactics to convince consumers that their computers were infected with viruses, spyware, or malware or had security breaches.

One ploy was to show consumers "Error" and "Warning" messages in the computer's Event Viewer and claim that these messages are indicative of viruses or other critical problems.[9] An FTC investigator encountered this tactic in the second of his three undercover calls to defendants' telemarketers.[10] Prior to the call, his computer was screened to ensure it was free of any "viruses, malware, spyware, or any

[9] *See* A1019-21; A1064-65; *see also* A307-08.

[10] A307-08.

other threats."[11] Nonetheless, defendants' telemarketer informed the investigator that "Error" and "Warning" messages displayed in the Event Viewer represented a "number of critical errors and warnings."[12] The telemarketer claimed there was no "option to delete" these errors and warnings,[13] but promised he would "get it done for [him]." A308. In actuality, as the FTC's expert explained, there were "no issues of concern on the system."[14] "[It] is normal for Windows systems to collect hundreds or thousands of such messages." A870.

Another ploy involved false representations that computer problems had caused certain Microsoft services and other programs to shut down or stop working.[15] For instance, in the second undercover call, the telemarketer falsely told the investigator that "critical errors

---

[11] A681 (FTC Information Technology Specialist performed a "clean install" and ran anti-virus software); A868 (FTC expert stating "[t]he system was in a nearly pristine state.").

[12] A307-08, 327 (screenshot of "Error" and "Warning" messages); *see generally* A866-67.

[13] A308, 329 (screenshot).

[14] A870. 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* A867.

[15] *See* A935; A942; A952; A1030-31; *see also* A307-08.

and warnings" displayed in Window's Event Viewer had caused "Stopped" services in System Configuration.[16] He also claimed that the "Stopped" services notice meant that "there are a lot of Microsoft services which are getting stuck day by day,"[17] and would have to be reactivated. A308.

The investigator encountered a similar ploy in his third undercover call. The telemarketer prompted System Configuration, which showed several "stopped services," and told the investigator that "a small glitch in the registry and some junk files" were causing the computer to run slowly.[18] In fact, the information displayed in System Configuration – including "Stopped Services" – was no sign that anything was wrong. A869. As the FTC's expert explained, "[i]t 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." *Id.*

Yet another deceptive ploy involved frightening consumers into believing that hackers were attempting to access or had already

[16] A308, 331 (screenshot of "Stopped" services).

[17] A308; *see generally* A746-47.

[18] A314-15; *see generally* A814.

accessed their computers.[19] For instance, in the second undercover call, this was accomplished by showing the investigator a number of "Untrusted" and "Fraudulent" certificates in the computer's Internet Properties and falsely claiming that these are evidence of hacking or security breaches. The telemarketer opened the web browser's Internet Properties, highlighted a number of "Untrusted" and "Fraudulent" website certificates[20] and then told the investigator, "[t]hese are the security breaches. Can you see that? Fraudulent, untrusted * * * [you] have a lot of fraud." A308. In actuality, those certificates did not indicate the presence of hackers or security breaches. They are merely an internal function of the web browser that discourages computer users from sending their information to untrusted web locations. A871.

---

[19] *See* A972 ("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."); A1010 ("They * * * showed me I had a foreign IP address and my identity could be stolen."); A1020 ("[H]e had my personal information on [the screen]. * * * [H]e said I got this information and that is how others can do it."); A1058 ("[They] were telling * * * that those hackers would be able to access my private information."); A1077 ("He said my system was so badly compromised that it was a matter of probably days before my entire identity would be stolen.").

[20] A308-09, 333 (screenshot of "Untrusted" and "Fraudulent" certificates in Internet Properties); *see generally* A748-49.

The telemarketers also used scare tactics with respect to other areas of the computer.[21] For example, during the first undercover call, the telemarketer prompted the computer's Prefetch folder and then falsely announced that "spam" was causing the computer to run slowly.[22] However, "spam" generally refers to unwanted email messages, and the Prefetch directory has nothing to do with email. Instead, it contains cached information designed to help the operating system to load programs more quickly. *See* A869-70. As the Commission's expert explained, the implication that files in the Prefetch directory are making the system run more slowly was "clearly false." A869-70.

The telemarketers used a similar ploy with respect to the computer's Temp folder. During the second undercover call, the telemarketer prompted the Temp folder and clicked on a text file. He then told the investigator, "You see that these are the viruses, malwares." A309. That, too, was false. The displayed text file was an installation log from the Symantec Endpoint Protection Suite. So rather than showing any viruses or malware on the system, the

[21] *See* A949; A963-64; A976; A1001; A1015; A1019; A1043; A1057-58.

[22] A305. A similar exchange occurred in Call Three. A314-15.

representative was actually displaying proof that software was installed on the system to help protect against these threats. A871.

To promote a quick sale, telemarketers created a false sense of urgency.[23] A skeptical consumer recalled telling a 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

[23] *See, e.g.*, A935 ("[They] had me convinced that the problem was serious and needed to be resolved ASAP."); A947 ("[H]e said a hacker had gotten into my system. Panicked, I believe [sic] him * * *."); A964 ("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."); A996 ("They made it sound really serious and tried to rush me into getting the 'hackers' off my 'network.'"); A1001 ("He intimidated me into and conned me into thinking that I was at severe risk for all my devices being compromised."); A1005 ("I was naïve but at the same time scared that I was being hacked so I agreed [to buy their services.]"); A1030-31 ("Panicked, I agreed * * * I was hesitant, and he pressured me for my credit card info."); A1034-35 ("I am by no means an advanced computer user and was scared that in fact my computer had been infected * * *."); A1043; A1052 ("I wanted to think about it but they scared me by saying these 'outside devices' could do some serious damage."); A1057-58 ("I was led to believe * * * that I needed a 'permanent' solution or that I would be at risk of identity theft * * *."); A1065-66 ("[I] was again presented with the "doomsday scenario" that my computer and router were infected."); A1072-73 ("It all seemed strange but quite honestly it scared [ ] me * * * I was desperate so I agreed."); A1077; A1081 ("[He] told me * * * someone hacked into my computer. * * * Of course, that made me panic."); A1111 ("I in fear reluctantly agreed * * *. ").

when he told me that my computer was at risk * * * [so] I agreed to pay Uber Tech Support to fix my computer." A1043.[24] Another consumer wanted "a day or so" to think about a purchase, but was told she could not call back. Fearful of losing her computer files and data, she paid for immediate "service." A1077.

Consumers who agreed to make a purchase were directed to one of defendants' websites where they paid from $199 to nearly $3000 for a one-time "repair" or long-term "support."[25] Telemarketers then transferred the remote session to technicians who purported to perform "repairs." *See, e.g.*, A312. In some instances, the technicians did not address the issue for which consumers sought help.[26] In other instances, the computer did not need the services prescribed.[27] One

---

[24] Uber Tech Support was a fictitious name adopted by defendants after the name "Click4Support" earned a bad reputation from its track record of consumer complaints.

[25] *See, e.g.*, A935 (charged $499); A942-43 ($2,797); A947 ($1,700); A949 ($599); A963 ($999); A970, 972 ($1,298); A1001 ($2,396); A1005 ($2,295); A1010 ($299); A1015 ($328); A1030-31 ($798); A1034-35 ($199); A1057-58 ($2,498); A1091 ($1,998); A1065 ($799); A1109, 1111 ($1,397).

[26] *See, e.g.*, A935 (printer); A947 (iPod); A970 (computer firewall); A1041 (phone); A1052 (printer); A1077 (router).

[27] *See, e.g.*, A993 ("When I later spoke to an actual Apple representative, the representative told me that it * * * the issue was with my TV, not

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 the Geek Squad told me that no viruses were in the computer * * *. [I]t was a 'clean' machine. * * * There was no problem, no virus infections, no need for repair."] A1015.

The FTC investigator encountered similar problems. In one undercover session, the telemarketer changed the Visual Effects settings of the investigator's computer and reset the virtual memory file size even though the FTC computer had no display performance issues and no shortage of disk space. A873-74. He also removed the security suite and replaced it with a different but functionally equivalent security program that provided "no improvement in the security of the

---

my computer."); A1010 ("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."); A1015; A1041 ("[A]fter working with the real Apple, I was informed there was no one trying to break into my computer * * *."); A1052 ("I never had any problems with my computer only my printer * * * * Bottom line there never was anything wrong with my computer.").

system."[28] There were in fact no security issues at the time of the undercover calls. A866.

Those "repairs" were not only unnecessary, in many instances they were also affirmatively harmful. Deleted files caused computer applications to launch "slightly slower."[29] Uninstalling a Maintenance Service program prevented automatic updates—including security patches—to the Firefox web browser.[30] Disabling several types of operating system warnings, including warnings about virus protection and automatic updates "hurt[] the overall security of the operating system." A875; s*ee* A134-35 (screenshots of technician disabling the warnings).

B. Formation of the Common Enterprise

To carry out this scheme, Gagneja needed merchant accounts to process consumers' credit card payments in the U.S. Without those

---

[28] A875 ("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*. A1005; A1010; A1072-73; A1101.

[29] A874. In some instances, defendants deleted consumers' important programs and files. *See, e.g.*, A949 ("My Wondershare software was completely deleted w/all my projects!!!"); A1072-73 ("Later I found out that they deleted my entire list of business phone numbers.").

[30] A874-75 ("[D]isabling the automatic update feature for Firefox hurts the overall security of the system rather than enhancing it.").

accounts, the scheme could not work. Gagneja contacted appellant George Saab and asked him to help set up credit card processing for his companies in return for a percentage of sales. A1267, A330.[31] Ultimately, the individual appellants, acting through their wholly owned company, Spanning Source LLC (Spanning Source), joined Gagneja's fraud. A1280. They formalized their unholy alliance in a Master Service Agreement signed on May 18, 2012. *See* A1399-1402, 1420-23; *see also* A1266-67; A1329-31.

Spanning Source began by opening a merchant account with TD Bank and registering a fictitious name in Pennsylvania – Click4Support.com. A1401. Defendants processed millions of consumer payments through this account until TD Bank terminated it for excessive "chargebacks" – *i.e.*, refunds that result when consumers dispute credit charges to their banks, as opposed to sellers. To keep the scheme going, Spanning Source opened a new merchant account with

[31] Gagneja initially tried to establish the merchant accounts through defendant Bruce Bartolotta, who was unable to secure the accounts. Bartolotta nevertheless incorporated the U.S. subsidiaries Innovazion-US and Click4Support LLC, paid for phone and some advertising services, and let Innovazion-U.S. and Click4Support use his Connecticut business address. Doc. 75 at 2; Doc. 76 at 2-3. Bartolotta is not a party to this appeal.

Chesapeake Bank. That account, too, was terminated for excessive chargebacks. *See* A292-93. Around the same time, the individual appellants opened a third account using the name of their other firm, iSourceUSA LLC (iSourceUSA). That account also collected millions of dollars from consumers. A1273 (Saab Decl.); A1336 (N. Patel Decl.); *see also* A1798-99; A1923.

As appellants opened new accounts and incorporated additional fictitious companies, the enterprise grew to include a maze of interrelated entities that shared a telephone number, offices, and employees, and commingled funds among bank accounts.[32] Initially, by agreement among the defendants, the plan was for Gagneja's companies to advertise, sell, and provide technical support services, while appellants' company – Spanning Source – would provide credit card processing through its own merchant account. *See*, *e.g.*, A1345-46; A1900. But credit card chargebacks soon mounted and in July 2013, Spanning Source took over responsibility for post-sale operations. The goal was to reduce chargebacks and thus avoid termination of the

[32] *See*, *e.g.*, A292-94 (shared telephone numbers and comingled funds); A1542-64 (shared workspace and comingled funds); A1824-25 (shared employees and comingled funds); A1879, 1904-05 (shared workspace and telephone numbers).

merchant accounts. A1902. From that point forward, Spanning Source was responsible for responding to consumer complaints and inquiries from state law enforcement officials. At offices leased by Gagneja's firm, Innovazion,[33] Spanning Source staff responded to requests for technical assistance and processed refund requests. A1824-25; A1900-04. Appellant Chetan Patel acted as the on-site supervisor at the office. Doc. 19 ¶¶ 33-34 (C. Patel Decl.). Appellant George Saab was involved in that effort as the "escalation point" person, even while working primarily from home. A1904. Chargebacks continued, however, and reached a point at which Spanning Source could no longer maintain its merchant accounts. A1824-25.

Appellants transferred much of their ill-gotten gains overseas.[34] From January 2013 to August 2014 alone, Spanning Source, iSourceUSA, and Innovazion-U.S. originated at least 73 wire transfers

[33] *See* A1542-47 (photos displaying business signs); A1549-51 (Bensalem Township records identifying Innovazion as lessee of offices used by iSourceUSA and Spanning Source); *see also* A1273 (Saab Decl.).

[34] *See* A577-78. Defendants iSourceUSA, Innovazion-U.S. and Spanning Source also transferred funds to each other. From May 2013 to November 2014, approximately $7 million flowed between and among these entities in 112 separate transactions. *Id*. *See also* A1554-57 (statements showing frequent deposits of funds by Spanning Source and iSourceUSA into Innovazion's bank account).

totaling over $4.6 million to Gagneja-owned accounts in India. *See* A577; Doc. 76 at 2 (Gagneja Decl.).

C. The Proceedings Below

On October 26, 2015, the FTC, joined by the State of Connecticut and the Commonwealth of Pennsylvania, filed an 11-count complaint charging appellants and others with engaging in unfair or deceptive practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), the FTC's Telemarketing Sales Rule (TSR), 16 C.F.R. Part 310, and various state consumer protection statutes. A101. The complaint (which was later amended to add additional defendants) named four corporate entities and four individuals.[35] The four original individual defendants are Bruce Bartolotta, who helped Gagneja launch his scheme in the U.S., and appellants George Saab, Chetan Patel (C. Patel), and Niraj Patel (N. Patel). The four original corporate defendants are Gagneja's

[35] By order dated May 5, 2016 (Doc. 105), the district court granted the Commission leave to file an amended complaint adding Abhishek Gagneja, his brother (Rishi Gagneja), and Innovazion-India as defendants.

companies, Click4Support, LLC[36] and Innovazion US,[37] and appellants Spanning Source[38] and iSourceUSA.[39]

To immediately halt the defendants' deceptive practices and preserve the possibility of effective final relief, the FTC moved for a preliminary injunction and simultaneously sought a TRO, asset freeze, and order appointing a temporary receiver for the corporate defendants. A184. To support its motion, the Commission submitted over 70 exhibits, including sworn declarations from (a) consumers; (b) representatives of U.S. technology companies; (c) an FTC investigator

---

[36] Click4Support is a Connecticut limited liability company. It was set up to offer helpdesk services, but never actually sold or marketed any tech support services. However, it received consumer complaints filed under its name (*see*, *e.g.*, A363), and responded to complaints. *See*, *e.g.*, A543-69. When Bruce Bartolotta received complaints filed against Click4Support he forwarded them to Spanning Source. *See* Doc. 75 at 2-3.

[37] Innovazion, Inc. was initially owned 100% by Abishek Gagneja. Defendant Bruce Bartolleta set it up as a Connecticut corporation in June 2011. Ultimately, it became a subsidiary of another Gagneja-owned firm, Innovazion Research Pvt. Ltd. Doc. 76 at 2.

[38] Spanning Source is a limited liability company owned by Saab, C. Patel, and N. Patel. Doc. 76 at 3.

[39] iSourceUSA was incorporated as a Pennsylvania limited liability company in August 2013. Spanning Source is the co-owner of iSource, and its principals retained control of the bank accounts and merchant bank relationship even after iSourceUSA took over credit card processing from Spanning Source. Doc. 76 at 4.

who, posing as a consumer, conducted and recorded three separate undercover calls; and (d) a computer and information security expert who analyzed those calls. The exhibits also included business documents obtained from third parties, such as financial institutions, representatives of the Better Business Bureau, telephone service providers and web hosting companies. *See* A226-73 (TRO Memorandum); A285-1116 (TRO Exhibit Lists and Exhibits); A1542-1603 (Supplemental Materials).

On October 27, 2015, the court issued a TRO, froze the assets of the individual and corporate defendants, appointed a temporary receiver, and scheduled a hearing on the motion for a preliminary injunction. A1129. The TRO specified that the motion for a preliminary injunction "shall be resolved on the pleadings, declarations, exhibits, and memoranda filed by, and oral argument of, the parties. Any arguments concerning the admissibility of the evidence shall go to the weight the Court shall give the evidence." A1165. The court also required that any request for live testimony be accompanied by (among other things) an "explanation of why the taking of live testimony would be helpful * * *." *Id*. Appellants did not object to these procedures.

The district court held a preliminary injunction hearing on November 9 and 10, 2015 (A1604-1954) and heard argument and live testimony from the individual appellants, N. Patel, C. Patel, and Saab. The court also heard the testimony of the FTC's investigator who, posing as a consumer during three separate calls, related the efforts of the India-based telemarketers to convince him that his computer was infected by viruses and malware or had experienced a security breach. A1639-61.

On November 10, 2015, the district court entered a preliminary injunction that in large part continued the prohibitions of the TRO and temporary receivership pending an adjudication on the merits. A37-68. Responding to claims of financial hardship, the court unfroze the individual appellants' personal assets. A45. The court also unfroze the assets and accounts of businesses "wholly unrelated" to the technical support services at issue. *Id*.

The district court applied the injunction standards relevant to public enforcement actions. A74-75. It concluded that the FTC was likely to succeed on the merits of its allegations that defendants, through a common enterprise, operated a deceptive technical services

scheme. A69-82. Not only did defendants falsely represent their affiliations with major tech companies, but, the court found, they also misrepresented the presence of malware and security breaches in consumers' computers. The court found that these claims were material to consumers' purchasing decisions because they were made "to explicitly lure consumers into paying for [their] services." A77.

Cautioning that its findings and conclusions had "no binding effect on the merits of [the] case" (A73), the court found that the corporate defendants operated as a common enterprise and therefore face "potential liability." A77. The court found that the defendants "transacted business through a maze of interrelated companies," with Gagneja's Click4Support and Innovazion providing tech support to consumers and appellant Spanning Source managing merchant accounts and processing refunds. A77-78. The court also pointed to the presence of other indicia of a common enterprise – common or shared owners, officers, and employees, shared addresses, websites, telephone numbers, and "at least" one bank account. A78.

The court also found that the individual appellants were likely personally liable for injunctive and monetary relief. *Id.* It noted they

had managed merchant accounts "without which the corporate defendants would not have been able to collect payments from consumers." *Id.* Indeed, the court relied on appellants' own sworn declarations and live testimony documenting the role of their closely held company in managing merchant accounts and processing refunds. A77-79. Furthermore, the court found, all three individual appellants likely "knew or were aware of the high probability of fraud" (A78), a conclusion that followed directly from their own testimony that the rate of chargebacks was so "extremely high" that "one of their bank accounts was closed." A78 & n.8. Given this evidence of control over the deceptive acts and their knowledge of at least a high "probability of fraud," the court concluded that the individual appellants "are likely to be held personally liable for their roles in th[e] enterprise." A79.

Balancing the equities, the court held that the individual appellants' private interests in continuing to operate their business were far outweighed by the public interest in "further prevent[ing] the defendants from separating consumers from their hard-earned money through deceptive practices." A81. On the other side of the scale, the

court held that the private equities are "significant for the individual defendants with regard to their asset freeze." A81.

Consistent with those findings, the court entered a preliminary injunction that essentially continued the prohibitions of the TRO and freeze of corporate assets pending a trial on the merits. A11-13. The court, however, lifted the freeze of the individual defendants' personal accounts, ruling that their need to pay living expenses and attorneys' fees was "significant." A79. Additionally, to protect consumers, the court also preliminarily restrained any party hosting a webpage or website and any domain registrar providing domain name registration for the corporate defendants from failing to take steps to prevent consumers from reaching defendants' offending websites or webpages. A10.

Spanning Source, C. Patel, N. Patel, and Saab appeal from entry of that order. A1.

SUMMARY OF ARGUMENT

Appellants participated in a scheme to induce consumers to call their telemarketers in India by using misleading internet ads and pop-up warning messages that appeared on consumers' computers. Once

they had consumers on the telephone, the telemarketers used false representations about their affiliation with well-known U.S. technology companies to convince consumers to allow them to remotely access their computers. After taking control over the computers, they scared consumers into believing that their computers were infected with viruses, spyware, or other malware, were being hacked, or were otherwise compromised. Then, they peddled their computer security or technical support services and charge consumers hundreds or even thousands of dollars for unnecessary services.

Because this scheme inflicted significant harm on unsuspecting consumers, the FTC and its co-plaintiffs, the Commonwealth of Pennsylvania and the State of Connecticut, filed a complaint alleging that appellants and others had violated the FTC Act, the FTC's Telemarketing Sales Rule, and various state consumer protection provisions. The FTC also sought preliminary relief to halt the scheme and to freeze assets and preserve evidence pending a disposition of the merits. The district court, finding that the FTC was likely to succeed on the merits of its claims and that the equities favored the issuance of

preliminary relief, granted the FTC's motion for a preliminary injunction and froze appellants' corporate assets.

The district court correctly found that the FTC is likely to succeed on the merits against appellants Spanning Source and its principals, George Saab, N. Patel, and C. Patel, who willingly joined and participated in the scheme to deceive consumers by providing a service that was necessary to make the scheme work – access to a merchant account to process consumers' credit card payments. In this appeal, appellants do not challenge the court's findings that the telemarketers used false statements about their affiliation with major technology companies to gain access to consumers' computers. They also do not seriously challenge the finding that the telemarketers made false representations about security and performance issues on consumers' computers, and that they used those misrepresentations to induce consumers to purchase unnecessary services.

Appellants deny, however, that they participated in a common enterprise. Instead, they allege, they engaged in an arms-length transaction with foreign telemarketers that resulted in an agreement to open and use merchant accounts in their own names as a means of

providing the telemarketers a means to accept credit card payments from U.S. consumers. The voluminous evidence before the district court, including appellants' own submissions and oral testimony, contradicts their assertion. Just one month after the telemarketing scheme launched, consumer complaints and the associated chargebacks alerted appellants about ongoing deception. Appellants' reaction to those alerts was not to quit or address those problems. Instead, they assumed new responsibilities, all with the goal to keep the scheme going and to maintain their share of net consumer sales.

There is no merit to any of the procedural issues raised by appellants. The district court properly received and considered the sworn declarations of consumers and the FTC's expert in consumer forensics. Any financial injury appellant suffered from the preliminary injunction follows necessarily from discontinuance of a scheme they do not deny was fraudulent. That private interest properly pales next to the paramount public interest in protecting U.S. consumers from deceptive practices.

STANDARD OF REVIEW

The scope of review of a district court order granting preliminary injunctive relief is particularly narrow. *See*, *e.g.*, *Delaware Strong Families v. Attorney General*, 793 F.3d 304, 308 (3d Cir. 2014); *Doe v. National Bd. of Medical Examiners*, 199 F.3d 146, 154 (3d Cir. 1999). This Court will overturn a grant of a preliminary injunction only if the district court "has abused its discretion, committed an obvious error in applying the law, or made a serious mistake in considering the proof." *United States v. Price*, 688 F.2d 204, 210 (3d Cir. 1982). While the district court's conclusions of law are subject to *de novo* review, its underlying factual findings are reviewed for clear error. *See*, *e.g.*, *New Jersey Retail Merchants Ass'n v. Sidamon-Eristoff*, 669 F.3d 374, 385 (3d Cir. 2012).

ARGUMENT

I. THE DISTRICT COURT PROPERLY ENJOINED APPELLANTS' UNLAWFUL CONDUCT AND FROZE CORPORATE ASSETS PENDING AN ADJUDICATION ON THE MERITS

Because Section 13(b) of the FTC Act empowers the district court to order a permanent injunction and monetary equitable relief, it authorizes such preliminary and ancillary relief as may be necessary to

ensure the availability of permanent relief. *FTC v. Gem Merch. Corp.*, 87 F.3d 466, 469 (11th Cir. 1996); *FTC v. Evans Products Co.*, 775 F.2d 1084, 1086 (9th Cir. 1985); *FTC v. U.S. Oil & Gas Corp.*, 748 F.2d 1431, 1433-34 (11th Cir. 1984).

Under Section 13(b) of the FTC Act, a court may issue an injunction "upon a proper showing that, weighing the equities and considering the [FTC]'s likelihood of ultimate success, such action would be in the public interest. . ." 15 U.S.C. § 53(b). The FTC need not demonstrate irreparable injury.[40] Rather, in determining whether to grant a preliminary injunction under Section 13(b), a court must (1) determine the likelihood the Commission will succeed on the merits; and (2) balance the equities. Harm to the public is presumed. *See*, *e.g.*, *FTC v. World Wide Factors, Ltd.*, 882 F.2d 344, 346 (9th Cir. 1989). Moreover, in balancing the equities, private equities are of secondary importance and are not sufficient, standing alone, to avoid an injunction. *World Wide Factors*, 882 F.2d at 347; *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1030-31 (7th Cir. 1988); *FTC v. Warner Communications, Inc.*, 742 F.2d 1156, 1165 (9th Cir. 1984).

[40] *See*, *e.g.*, *World Wide Factors, Ltd.*, 882 F.2d at 347; *World Travel Vacation Brokers, Inc.*, 861 F.2d at 1029.

A. The FTC Is Likely to Succeed in Showing that Appellants Participated in a Common Enterprise

1. Appellants Do Not And Cannot Dispute the Overwhelming Evidence of Their Involvement

Appellants do not dispute that the telemarketers made deceptive representations about their affiliations and then used those misrepresentations to gain access to consumers' computers. Nor do they dispute that those and other misrepresentations lured consumers into buying unnecessary support services. Nor do they dispute that – in return for a percentage of sales – they processed credit card payments, responded to requests for refunds, and provided other post-sale "technical assistance."

Appellants' argument that they are not liable for any deception misconstrues the common enterprise doctrine, ignores the evidence presented by the FTC, and is belied by their own submissions. Courts consider a number of factors in identifying a common enterprise. Whether defendants share office space, engage in interrelated activities, commingle funds, maintain common employees, operate under common control, and share telephone numbers are all relevant inquiries and are all present here in varying degrees. *See*, *e.g.*, *FTC v. Network Servs.*

Depot, 617 F. 3d 1127, 1142-43 (9th Cir. 2010); *FTC v. E.M.A. Nationwide, Inc.*, 767 F.3d 611, 637 (6th Cir. 2014).

But the *crux* of the inquiry is whether defendants acted together in furtherance of a common scheme. "[E]ntities constitute a common enterprise when they exhibit either vertical or horizontal commonality—qualities that may be demonstrated by a showing of strongly interdependent economic interests or the pooling of assets and revenues." *Network Servs. Depot*, 617 F.3d at 1142-43.[41]

The evidence here satisfies that standard. Appellants maintained a critical and central role in the technical support scam over a sustained period of time. Ganeja and his companies (Innovazion-India and Innovazion-U.S.) could not have defrauded consumers of their money without appellants' active contributions. Appellants' willingness to undertake their role not only allowed the scheme to succeed initially, but also enabled it to grow even in the face of chargebacks and consumer complaints.

---

[41] Other courts have similarly described such strongly interdependent economic interests as a "joint venture," and held the joint venturers directly liable for consumer harm. *See*, *e.g.*, *FTC v. Direct Mkt'g Concepts, Inc.*, 569 F. Supp. 2d 285, 309-10 (D. Mass. 2008), *aff'd on other grounds*, 624 F.3d 1 (1st Cir. 2010).

Appellants continued to participate even after TD Bank terminated its account for persistent high chargebacks. At that juncture, appellants could have quit. They did not. Instead, they increased their participation in the scheme. They created a chargeback reduction and business improvement plan that was designed not to address the deceptive representations, but to reduce chargeback levels and thereby preserve their share of net consumer sales. *See*, *e.g.*, A1270-72. When those efforts failed to prevent termination of their account by their merchant bank, appellants pursued banks with a greater tolerance for high chargebacks, thus ensuring that the deceptive practices would persist unabated. *See*, *e.g.*, A1273-75. Ultimately, appellants and Gagneja resorted to using another firm owned by appellants – iSourceUSA – to open yet another merchant account.[42] Complaints and chargebacks continued, however, despite appellants' efforts to "save" sales and reduce chargebacks. A1274.

Appellants' suggestion that they operated at arms-length from the telemarketers in India is belied by their response to TD Bank's threatened termination of their merchant account. At that point,

[42] The new Operating Agreement reflected Spanning Source's 60% share and Innovazion's 40% share of iSourceUSA. A1273.

instead of quitting, they assumed new responsibilities and opened new merchant accounts. The goal was to save sales and, by granting direct refunds to consumers, to ensure they would not request chargebacks from their banks. *See*, *e.g.*, A1811; *see also* A1270-71, 1274-75. That conduct was designed to ensure they would continue to benefit from the fraudulent sales. It is far from the disinterested, arms-length relationship that appellants try to portray. The record amply supports the district court's conclusion that the FTC is likely to prove that appellants participated in a common enterprise.

2. The District Court Applied the Correct Legal Standard in Finding the FTC Had a "Likelihood of Success"

The proper inquiry is whether the FTC demonstrated a "likelihood of success" on the merits. *See*, *e.g.*, *FTC v. Trek Alliance*, 81 F. Appx. 118, 118 (9th Cir. 2003); *World Wide Factors*, 882 F.2d at 346; *World Travel Vacation Brokers, Inc.*, 861 F.2d at 1024. The district court found that it did, and as described above, the evidence amply supports that finding.

Rather than dispute this evidence, appellants contend that a more stringent standard was required – that, before granting preliminary

injunctive relief, the court should have found that the evidence of common enterprise was "indisputably clear." Br. 34. Appellants' rationale is twofold: (1) that the court issued a mandatory injunction – *i.e.*, an order that commands a positive act; and (2) the injunction issued by the court altered the status quo. In such circumstances, they contend, a heightened standard should apply. Br. 33-34.

But the distinction between mandatory and prohibitive injunctions does not help appellants because it is often a matter of semantics. Injunctive provisions containing essentially the same command can usually be cast in either mandatory or prohibitive terms. *See Tom Doherty Associates, Inc. v. Saban Entertainment, Inc.*, 60 F.3d 27, 34 (2d Cir. 1995).

Even so, it is difficult to understand appellants' grievance because the principal operative provisions of the order at issue are cast in prohibitive – not mandatory – terms. A40-42. This order is thus very different from orders where the mandatory terms required affected parties to undertake costly and ongoing programs. *See, e.g., Trinity Indus., Inc. v. Chicago Bridge & Iron Co.*, 735 F.3d 131 (3d Cir. 2013) (clean up an environmental hazard); *see also Tom Doherty Assocs., Inc.*

v. Saban Entertainment, Inc., 60 F.3d 27 (2d Cir. 1995) (compulsory licensure of publishing rights). Indeed, unlike the cases appellants cite, the order here requires no expenditure of funds or other effort at all.

Appellants' grievance thus focuses on the *effect* of the order, which they assert was to put them out of business, "causing a great financial loss of investment and profit." Br. 33. According to appellants, this was error because "[t]his was not a mere preservation of the status quo." *Id.* But a district court is not obliged to maintain the status quo when the status quo is "a condition of action, which, if allowed to continue or proceed unchecked and unrestrained, will inflict serious irreparable injury." *Price*, 688 F. 2d at 212. Rather, a district court, sitting in equity, may fashion any remedy that is appropriate to do justice. *Id.* at 211. That is precisely the situation faced by the district court in this case, when the FTC presented evidence of ongoing deceptive practices that, unless stopped immediately, would cause consumers to incur continued losses pending an adjudication on the merits.

Even if a heightened standard applied, the FTC satisfied it. The conclusion that appellants participated in a common enterprise follows directly from their own submissions to the district court, including the

appellants' live and written testimony. The FTC's submissions, which included numerous sworn declarations of injured consumers and tech company officials, provide additional supporting evidence of appellants' wrongdoing. Appellants dismiss this evidence as "hearsay" (Br. 38-40), but such evidence is appropriate to consider in preliminary injunction proceedings. Such proceedings "are less formal" and call for "evidence that is less complete than in a trial on the merits." *Univ. of Texas v. Camenisch*, 451 U.S. 390, 395 (1981). Indeed, this Court and others have uniformly approved reliance on hearsay in determining whether to award a preliminary injunction. *See Kos Pharms., Inc. v. Andrx Corp.*, 369 F.3d 700, 718 (3d Cir. 2004); *Adams v. Freedom Forge Corp.*, 204 F.3d 475, 487 (3d Cir. 2000).[43] A district court has a considerable measure of discretion in admitting sworn declarations in lieu of live testimony even in a trial on the merits. *See, e.g.*, *FTC v. Amy Travel Service, Inc.*, 875 F.2d 564, 576 (7th Cir. 1989).

[43] *Accord Mullins v. City of New York*, 626 F.3d 47, 51-52 (2d Cir. 2010); *Ty, Inc. v. GMA Accessories, Inc.*, 132 F.3d 1167, 1170-71 (7th Cir. 1997); *Levi Strauss & Co. v. Sunrise Int'l Trading, Inc.*, 51 F.3d 982, 985 (11th Cir. 1995); *Sierra Club v. FDIC*, 992 F.2d 545, 551 (5th Cir. 1993); *Asseo v. Pan Am. Grain Co.*, 805 F.2d 23, 26 (1st Cir. 1986); *Flynt Distrib. Co.. v. Harvey*, 734 F.2d 1389, 1394 (9th Cir. 1984).

The relevant question is not whether such evidence is hearsay, but whether – considering the need for haste (in light of ongoing injuries) and the reliability of the information – "the type of evidence was appropriate given the character and objectives of the injunctive proceeding." *Asseo v. Pan Am. Grain Co.*, 805 F.2d 23, 26 (1st Cir. 1986). It plainly was. The interests of justice were served by allowing the declarants to submit sworn declarations instead of making a personal appearance in court. Given the nationwide scope of the scheme and the need to act quickly, it was not practicable to require the appearance of consumer declarants in court. *See Amy Travel Service*, 875 F.2d at 576; *FTC v. Kitco of Nevada, Inc.*, 612 F. Supp. 1282, 1294 (D. Nev. 1985). Furthermore, the declarations were made under oath and describe facts about which the declarants have personal knowledge – *e.g.*, for the consumer declarants, their contacts with the defendants. Appellants offer no reason to question their trustworthiness. *See Amy Travel Service*, 875 F.2d at 576. Indeed, such statements are admissible under the residual exception in Rule 807 of the Federal Rules of Evidence.[44]

[44] For the same reasons, appellants are wrong when they claim that the

In any event, as we have noted, appellants do not challenge the truthfulness of the record evidence. Equally important, they voiced no objections to the procedures announced in the TRO. Indeed, they failed to raise them at any time in advance of the scheduled hearing. Given this failure to raise the issue with the district court in a timely fashion, they may not raise it now. *See*, *e.g.*, *K-Mart v. Oriental Plaza, Inc.*, 875 F.2d 907, 913-14 (1st Cir. 1989). The court's unchallenged decision to admit and rely on sworn declarations was not an abuse of discretion.

3. Appellants' Allegations of Procedural Error Are Meritless

Appellants also contend that three procedural errors mandate reversal of the preliminary injunction, but these claims fail as well.

a. The district court properly considered the expert declaration.

Appellants assert that the district court erred in receiving the sworn declaration of the FTC's expert in computer forensics in lieu of his live testimony. Br. 44. According to appellants, the expert's testimony was the "linchpin that married the alleged consumer complaints to the alleged wrongdoing * * *." *Id.* Therefore, they claim,

---

FTC's expert's declaration should not have been admitted.

they were "very much prejudiced" when the FTC did not call him as a witness. *Id.*

The claim is wrong. The link between the consumer complaints and the alleged wrongdoing was the live testimony of the FTC investigator, who reviewed hundreds of consumer complaints and the declarations of 29 sworn consumer declarants. During the hearing, the investigator described the common themes in those complaints and declarations and their description of the telemarketers' unlawful conduct. *See* A1661-65, 1670-71. The guts of the FTC's case lie in these consumer documents, which were also part of the record before the district court.

Thus, the testimony of the FTC's expert, while valuable in its methodical presentation, is not the "linchpin" of the FTC's case. The FTC investigator knew at the time of his calls that his computer was in "pristine condition," free of viruses, malware, or security breaches. A1635. He did not need to rely on the expert declaration to understand the fraud.

Furthermore, nothing in *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), on which appellants rely, requires a district

court to act *sua sponte* to convene a hearing to examine an expert's credentials. Here, appellants did not challenge the FTC's expert's credentials. Nor do they say how such a hearing would have advanced their position. In any event, the expert's sworn declaration was already before the court. In those circumstances, more was not required. *See*, *e.g.*, *Henry v. St. Croix Alumna, LLC*, 572 Fed. Appx. 114, 118-19 (3d Cir. 2014).

b. The district court's decision to proceed without a full-scale hearing was proper and unchallenged by appellants.

Finally, appellants fault the district court for failing to conduct a full-scale evidentiary hearing. Br. 37-46. The claim is both waived and wrong. When it entered the TRO on October 27, 2015, the district court described in detail the procedures it would use to evaluate the FTC's motion for a preliminary injunction. *See* A1164-65. The court directed the parties to notify the court and opposing counsel of any request for live testimony no later than four days before the motion hearing. *Id.* A month later, the court held a status conference at which it reviewed those procedures with the parties. At no time did appellants object to the court's procedures. They may not challenge them now.

Appellants identify no error in the district court's chosen procedures in any event. The court suitably balanced defendants' interests with the need to act quickly to protect consumers from ongoing harm. Indeed, the district court was entitled to resolve the motion for a preliminary injunction on the basis of written submissions alone. *See*, *e.g.*, *Bradley v. Pittsburgh Bd. of Educ.*, 910 F.2d 1172, 1175-76 (3d Cir. 1990). The court nevertheless allowed appellants to present live witnesses, including appellants Saab, C. Patel and N. Patel. *See* A1610.

c. The district court properly issued its findings of fact and conclusions of law in memorandum opinion form

Apparently fearing reputational harm, appellants attack the district court for preparing a memorandum decision that third parties might construe as a final ruling on the allegation that appellants were part of a common enterprise. Br. 25-29. This strains credulity, considering that the district court plainly stated that the proceeding was "a preliminary injunction hearing with no binding effect on the merits of the case." A73. Appellants seem to disagree not with anything the court said, but with what others may take away from it. That is not a ground for reversal.

Fed. R. Civ. 52(a)(2) requires a district court, in granting an interlocutory injunction, to clearly state the findings and conclusions that support its action. *See also* Fed. R. Civ. P. 65(d)(1). By stating its findings and providing supporting references in the record, the district court adhered to those requirements. Had the district court failed to provide this Court with the factual premise of its ruling, that might have been error. Indeed, in the very case on which appellants rely, *PharMethod v. Caserta*, 382 F. App'x 214, 218 (3d Cir. 2010), this Court vacated a preliminary injunction precisely because the "paucity of findings of fact and conclusions of law" provided an "insufficient basis for meaningful appellate review."

B. The District Court Correctly Gave Greater Weight to the Public Interest

Appellants assert that the district court did not properly balance the equities. In particular, they contend that even if they prevail on the merits, they will have suffered irreversible damage to their reputations and their ability to resume merchant account operations. Br. 32-35. They also object to order provisions that require third parties who host defendants' consumer-facing websites to suspend the websites pending

an adjudication of the merits – a step needed to protect consumers from continuing harm by unnamed participants.[45] *See* Br. 36.

Having found that the FTC was likely to establish that appellants deceived consumers, the court rightly concluded that that the public interest in ending deception outweighed appellants' private interests in continuing the deception. "[T]he public interest, when in conflict with private interest, is paramount." *CFTC v. British American Commodity Options Corp.*, 560 F.2d 135, 143 (2d Cir. 1977). Appellants' concerns about their reputations are speculative, and in any event do not constitute cognizable legal injury in this context. *See*, *e.g.*, *Sampson v. Murray*, 415 U.S. 61, 89 (1974); *Hunter v. Hirsig*, 614 F. App'x 960, 963 (10th Cir. 2015); *Franks v. Nimmo*, 683 F.2d 1290, 1294 (10th Cir. 1982).[46] Such allegations could be made in response to nearly every government enforcement action, leading to a virtual per se ban on injunctive relief. That is not the law.

---

[45] Leaving the websites open and active pending adjudication on the merits would expose consumers to harm from third-party scammers posing as Click4Support. In fact, defendants have complained that they are "victims" of such scammers. *See*, *e.g.*, Doc. 76 at 7-8 (Gagneja declaration).

[46] To the extent appellants qualify, however, they may have a claim under the Equal Access to Justice Act, 28 U.S.C. § 2412.

CONCLUSION

For all the foregoing reasons, the judgment of the district court should be affirmed.

Respectfully submitted,

DAVID C. SHONKA
Acting General Counsel

JOEL MARCUS
Director of Litigation

*/s/*Leslie Rice Melman
LESLIE RICE MELMAN
Assistant General Counsel

FEDERAL TRADE COMMISSION
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580
(202) 326-2478

Of Counsel:
JON M. STEIGER
Director, East Central Region

FIL M. DE BANATE
CHRISTOPHER D. PANEK
Attorneys
FEDERAL TRADE COMMISSION
Cleveland, OH 44114

CERTIFICATE OF COMPLIANCE WITH VOLUME LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS

I. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because the brief contains 9,203 words

II. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word, 2010, 14-point Century Schoolbook.

/s/ Leslie Rice Melman

July 6, 2016

CERTIFICATE OF PERFORMANCE OF VIRUS CHECK

I certify that on July 6, 2016, I performed a virus check on the electronically filed Addendum to Brief of the Federal Trade Commission using Symantec Endpoint Protection, version 12.1.6 (12.1 RU6 MP4) build 6867 (12.1.6867.6400). No virus was detected.

/s/ Leslie Rice Melman

July 6, 2016

CERTIFICATE OF SERVICE

I certify that on July 6, 2016, I filed the foregoing Addendum to Brief of the Federal Trade Commission via the Court's electronic filing system. All parties have consented to receive electronic service and will be served by the ECF system.

/s/ Leslie Rice Melman