No. 18-56161

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

FEDERAL TRADE COMMISSION,
Plaintiff-Appellee,

v.

HARDWIRE INTERACTIVE, INC.,
Defendant-Appellant.

On Appeal from the United States District Court
for the Southern District of California
No. 3:18-cv-01388-MMA-NLS
Hon. Michael M. Anello

ANSWERING BRIEF FOR THE FEDERAL TRADE COMMISSION

ALDEN F. ABBOTT
General Counsel

JOEL MARCUS
Deputy General Counsel

OLGA VAYTSMAN
MICHELE ARINGTON
Attorneys

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
(202) 326-3626
ovaytsman@ftc.gov

Of Counsel:
SAMANTHA GORDON
MATTHEY H. WERNZ
Attorneys

FEDERAL TRADE COMMISSION
230 S. Dearborn Street, Suite 3030
Chicago, IL 60604

TABLE OF CONTENTS

Table of Authorities iii

Jurisdiction 1

Questions Presented 1

Statement of the Case 2

A. Hardwire's Deceptive Marketing Scheme. 4

B. Hardwire's Scam Was Based in the United States. 7

C. The SAFE WEB Act 10

D. The FTC's Enforcement Lawsuit And The Preliminary Injunction 14

Summary of Argument 18

Standard of Review 22

Argument 22

I. The District Court Properly Enjoined All Of Hardwire's Fraudulent Practices, Foreign And Domestic 23

A. The District Court Correctly Found That Hardwire's Foreign Business Operations Likely Involved Material Domestic Conduct And Were Likely To Harm U.S. Consumers 24

B. Hardwire Fails To Refute The Substantial Evidence Of Material Domestic Conduct 30

II. The District Court Properly Exercised Its Discretion In Determining The Scope Of Preliminary Injunctive Relief. 36

A. The District Court Could Properly Enjoin Hardwire's Foreign Fraudulent Practices Notwithstanding The Promise To Sever U.S. Connections 37

B. The District Court Properly Considered Less Restrictive Alternatives 40

Conclusion 43

TABLE OF AUTHORITIES

CASES

Branch v. FTC, 141 F.2d 31 (7th Cir. 1944) 10

Conservation Cong. v. U.S. Forest Serv., 720 F.3d 1048 (9th Cir. 2013).....22

F. Hoffmann-La Roche Ltd. v. Empagran S.A., 542 U.S. 155 (2004)..... 34, 35, 36

FTC v. Affordable Media, LLC, 179 F.3d 1228 (9th Cir. 1999)..... 22, 38

FTC v. Atkinson, 1:08-cv-05666 (N.D. Ill., filed Oct. 6, 2008) 13

FTC v. Grant Connect, LLC, 763 F.3d 1094 (9th Cir. 2014)..... 26, 39

FTC v. Innovative Marketing, Inc., No. 1:08-cv-03233-RDB (D. Md., filed Dec. 2, 2008).....13

FTC v. Nat'l Lead Co., 352 U.S. 419 (1957) 40

FTC v. PCCare247 Inc., No. 1:12-cv-07189-PAE (S.D.N.Y., filed Sept. 24, 2012).....14

FTC v. Willms, No. 2:11-cv-00828-MJP (W.D. Wash., filed May 16, 2011) 12, 13

Johnson v. Couturier, 572 F.3d 1067 (9th Cir. 2009) 22

M.R. v. Dreyfus, 697 F.3d 706 (9th Cir. 2012) 22

SEC v. International Swiss Investments Corp., 895 F.2d 1272 (9th Cir. 1990).....40

United States v. E.I. du Pont de Nemours & Co., 366 U.S. 316 (1961).....36

United States v. First Nat'l City Bank,
379 U.S. 378 (1965) 40

United States v. Oregon State Med. Soc.,
343 U.S. 326 (1952) 38

STATUTES

Electronic Fund Transfer Act

15 U.S.C. § 1693e(a) 3

15 U.S.C. § 1693o(c) 23

Federal Trade Commission Act ("FTC Act")

15 U.S.C. § 45(a) 1, 3, 12, 18, 23, 35

15 U.S.C. § 53(b) 1

Foreign Trade Antitrust Improvements Act ("FTAIA")

15 U.S.C. § 6a 35

Restore Online Shoppers Confidence ("ROSCA")

15 U.S.C. § 8403 3

15 U.SC. § 8404(a) 1, 23

Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 ("SAFE WEB Act")

Pub. L. No. 109-455, 120 Stat. 3372 (2006) 11

28 U.S.C. § 1292(a)(1) 1

28 U.S.C. § 1331 1

28 U.S.C. § 1337(a) 1

28 U.S.C. § 1345 1

RULES AND REGULATIONS

12 C.F.R. § 205.10(b) 3

OTHER AUTHORITIES

Fed. Trade Comm'n, *The US SAFE WEB Act: Protecting Consumers from Spam, Spyware, and Fraud – A Legislative Recommendation to Congress* (2005).....11

JURISDICTION

The district court had jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), 1345; 15 U.S.C. §§ 45(a), 53(b); and 15 U.S.C. § 8404(a). The district court entered a preliminary injunction against all defendants on August 24, 2018, and appellant Hardwire Interactive, Inc. timely filed a notice of appeal on August 27, 2018.

This Court has jurisdiction pursuant to 28 U.S.C. § 1292(a)(1).

QUESTIONS PRESENTED

In 2006, Congress granted the Federal Trade Commission ("FTC" or "Commission") authority to combat fraud committed in foreign countries and to secure redress for defrauded foreign consumers so long as the foreign violations "cause or are likely to cause reasonably foreseeable injury within the United States" or "involve material conduct occurring within the United States." 15 U.S.C. § 45(a)(4)(A)(i)-(ii).

Hardwire and other companies, operating as a single, integrated common enterprise with its hub in the United States, ran a multinational deceptive marketing scheme that bilked U.S. consumers of more than $50 million during 2017-2018 alone and foreign consumers of millions more. The district court found that Hardwire's scheme relied on extensive material conduct in the United States, including the purchase of telecommunications services, website services,

marketing services, and payment processing services. In addition, the court found that Hardwire's international business is entwined with its U.S.-based operations as a common enterprise, such that there is no genuine distinction between the foreign and domestic operations. The court found further that Hardwire's overseas operations posed a risk of harm to U.S. consumers. The district court issued a preliminary injunction prohibiting Hardwire from continuing its fraudulent practices worldwide and freezing its assets to preserve them for consumer redress.

The questions presented are:

1. Whether the FTC Act authorized the court to preliminarily enjoin Hardwire's fraudulent conduct without geographic limitation, where its operations abroad were part of an integrated, U.S.-based enterprise that has injured U.S. consumers and involved material conduct within the United States.

2. Whether the district court abused its discretion in declining to limit the preliminary injunction so that Hardwire could continue its deceptive business practices with respect to persons located outside of the United States.

STATEMENT OF THE CASE

Hardwire and its co-defendants ran a deceptive online marketing scheme. They baited consumers over the internet with offers of "risk-free" product trials for only the cost of shipping, but in fact charged them in full for multiple products and enrolled them in "continuity" programs with recurring monthly charges. The

victims neither were clearly informed of nor knowingly consented to those charges. Consumers unwittingly agreed to additional charges by virtue of a hidden "negative option" feature on Hardwire's website, which deemed the consumer's silence as acceptance of enrollment in the continuity program.

The Commission sued Hardwire and its co-defendants under laws enforced by the Commission that ensure that merchants act honestly and that consumers will have adequate information to make a knowing and informed consent to recurring charges before they are imposed. Section 5(a) of the FTC Act prohibits "unfair or deceptive acts or practices." 15 U.S.C. § 45(a). The Restore Online Shoppers' Confidence Act ("ROSCA") prohibits negative option billing for online sales without clear disclosures, express consent, and a simple means to stop recurring charges. 15 U.S.C. § 8403. The Electronic Fund Transfer Act ("EFTA") and its implementing rule, known as Regulation E, require written authorization before merchants may make regularly recurring debits from a consumer's bank account. 15 U.S.C. § 1693e(a); 12 C.F.R. § 205.10(b).

The district court entered a Temporary Restraining Order ("TRO"), followed by a preliminary injunction, placing the corporate defendants under receivership and freezing their assets to preserve them for consumer redress. As described below, the court ruled that the FTC Act reaches the defendants' foreign business and rejected Hardwire's request for permission to continue its deceptive marketing

practices outside of the United States. The court found that the FTC Act applies to Hardwire's international activities because they are intertwined with its domestic operations and relied on services provided domestically, and thus amounted both to material conduct in the United States and conduct likely to cause injury in the United States.

A. Hardwire's Deceptive Marketing Scheme

Hardwire sold a variety of products—skin care creams, electronic cigarettes, and dietary supplements—over the internet. Dkt. 30-12 Exh. 11 at 6-11 [SER0108-13].[1] It lured consumers to its product websites through social media, emails, YouTube videos, and other forms of online advertising that offered a "risk free" trial of the products. *See, e.g.*, PX10 ¶37, Att. I at 304 [ER0456, 0585]; PX10 ¶62, Att. J at 325-26 [ER0464, 0604-05]; PX10 ¶79, Att. K at 353 [ER0470, 0632]; PX10 ¶102, Att. M at 382-94 [ER0478-79, 0661-73]; PX10 ¶¶108-09, Att. N at 404-22 [ER0481, 0683-701]; PX10 ¶¶114-16, Att. O at 439-62 [ER0483-84, 0718-41]. The websites represented that the offer was risk free because consumers had only to pay a small shipping and handling fee (typically $4.95). *See, e.g.*, PX10 Att. H at 278-79 [ER0559-60]; PX10 Att. I at 312 [ER0593]; PX10 Att. J at 334

[1] "Dkt. [#]" refers to the district court's docket number; page number citations within the document are to the PDF pagination. "PX" refers to Plaintiff's Exhibit; page number citations are to the PX pagination. "Br." refers to appellant's Brief. "ER" refers to appellant's Excerpts of Record. "SER" refers to the FTC's Supplemental Excerpts of Record, filed herewith.

[ER0613]; PX10 Att. K at 360 [ER0639]; PX10 Att. P at 507-08 [ER0786]. Consumers were asked to provide credit or debit card information—ostensibly to pay the shipping fee—and directed to click a check-out button that read "GET MY RISK FREE TRIAL" (or "CONTINUE" or some other variant). *See, e.g.*, PX10 Att. H at 278-79 [ER0559-60]; PX10 Att. I at 312 [ER0593]; PX10 Att. J at 334 [ER0613]; PX10 Att. K at 360 [ER0639]; PX10 Att. P at 507-08 [ER0786].

In reality, clicking the button secretly authorized Hardwire to charge consumers the full price of the purported "risk free" product—as much as $100—and then enrolled them in a continuity plan of recurring monthly product shipments and associated charges. *See, e.g.*, PX10 ¶53 [ER0461]; PX10 ¶65, Att. J at 334 [ER0465-66, 0613]; PX10 ¶82, Att. K at 360 [ER0471-72, 0639]; PX10 ¶126, Att. P at 507-08 [ER0487-88, 0786-87]. Those terms and conditions, including the need to immediately cancel the "trial" to avoid the later charges, were concealed in barely legible fine print at the bottom of the payment page, well below where consumers entered their billing information and clicked the check-out button. *See, e.g.*, PX10 ¶65, Att. J at 334 [ER0465-66, 0613]; PX10 ¶126, Att. P at 507-08 [ER0487-88, 0786-87].[2] The disclosures may not have been visible on the payment

[2] In some cases, the only disclosures provided were buried in a separate "Terms and Conditions" page accessible via a faint hyperlink. *See, e.g.*, PX10 ¶40, Att. I at 310, 312 [ER0457-57, 0591, 0563]. Consumers could complete the transaction without ever having clicked on this hyperlink. PX10 ¶41 [ER0458].

page at all to consumers using a mobile device. *See, e.g.*, PX10 Att. N at 435-36 [ER0714-16]. As a result, consumers did not even see these disclosures, let alone read them.

To make matters worse, Hardwire's websites tricked consumers into ordering a second "trial" product. After consumers entered their billing information and clicked the "GET MY RISK FREE TRIAL" button, they were routed to a webpage falsely indicating that the order was not yet complete. There, they were presented with a "COMPLETE CHECKOUT" button, located under an advertisement for another product, that when clicked unwittingly signed them up for a "trial" of the other product. *See, e.g.*, PX10 ¶19, Att. H at 280-81 [ER0449-50, 0561-62]; PX10 ¶¶42, 43, Att. I at 313 [ER0458-59, 0594]; PX10 ¶¶67, 68, Att. J at 335 [ER0466-67, 0614-15]. Soon after, consumers were charged the full price for this additional "trial" product and enrolled in another monthly continuity plan. *See, e.g.*, PX10 ¶19 [ER0449-50]. As with the initial "risk free" trial offer, the true terms of the deal were buried far below the "COMPLETE CHECKOUT" button in barely legible fine print. *See, e.g.*, PX10 ¶19, Att. H at 280-81 [ER0449-50, 0561-62].

Thus, the "risk free" trial for which a consumer authorized only a $4.95 charge often resulted in charges of more than $200 in the first month alone and ongoing charges after that. *See, e.g.*, PX6 ¶8 [ER0989-90]. Many consumers who

discovered these unauthorized charges and sought refunds were unable to get their money back because of Hardwire's restrictive refund policies. *See, e.g.* PX1 ¶¶8-11 [ER0896-97]; PX5 ¶¶8-12 [ER0978-80]; PX6 ¶¶7-9 [ER0989-90]. In 2017 and 2018 alone, the scam stole more than $50 million from victims in the United States, and it had been ongoing for several years before that. Dkt. 30 at 24 [SER0088]; PX11 ¶39 [SER0208]. Hardwire deceived foreign consumers too. It used the same deceptive tactics and nearly identical websites to run the scam on victims abroad, stealing millions more from them. *Compare* PX10 Att. J at 327-34 [ER0606-13] (U.S. website) *with* PX11 Att. K at 120-27 [SER0255-62] (U.K. website); *see also* Dkt. 30 at 24-25 [SER0088-89].

B. Hardwire's Scam Was Based in the United States

The deceptive marketing scheme was the brainchild of Devin Keer, Hardwire's principal, and his long-time friend and business partner Brian Phillips, Triangle Media's principal.[3] Dkt. 30 at 16 [SER0080]. They have been executing variants of the "risk free trial" scam since 2008, starting with a Texas-based business that ultimately shut down after excessive consumer complaints. *Id*.

[3] Keer is not a named defendant because the FTC did not learn of the full extent of his involvement until after it filed the complaint and gained access to corporate documents. FTC counsel has informed the district court that based on evidence uncovered since the filing of suit, it intends to seek leave to amend the complaint to add Keer as a defendant. Dkt. 28 at 14 n.26.

Keer and Phillips have operated the present incarnation of the scheme since at least 2013 through Hardwire, Triangle Media, and a warren of other companies operating as a single entitiy. PX11 ¶39 [SER0208] (describing consumer complaints dating back to 2013); Dkt. 30 at 5 [SER0069]. Hardwire handled marketing and sales (Br. 7-8); Triangle Media provided critical back-office support functions. PX11 ¶14, Att. G at 43-60 [SER0197, 0223-40] (monitoring call centers); Dkt. 30 at 12, 16 [SER0076, 0080] (managing shell merchant accounts). The companies were commonly owned and controlled by Keer and Phillips, shared personnel (including one who held himself out both as Hardwire's general manager and Triangle Media's COO), and commingled funds, all towards the same fraudulent end. Dkt. 30 at 16-21 [SER0080-85]; PX10 ¶¶9-10 [ER0445]. Because the companies disregarded corporate formalities, the district court found them to be a "common enterprise" jointly liable for each other's unlawful activities. Dkt. 74 at 20-24 [ER0048-52].

The enterprise was centered in the United States. Triangle Media is a U.S. company. PX10 ¶5 [ER0043-44]. The scheme used a U.S.-based domain registrar (Wild West Domains) to register domain names for its websites—including sites directed at foreign consumers—and a U.S. provider (Amazon Technologies) to host those websites. PX10 ¶132 [ER0491-93]; PX11 ¶¶19, 21 [SER0200]; *see also infra* note 14 (explaining that foreign websites were often part of the same domain

as the domestic ones). Hardwire used a U.S.-based online marketing network (Clickbooth.com) to advertise its misleading "free trial" claims—to consumers in the U.S. and abroad—and drive consumers to its websites. PX11 ¶17, Att. J at 107-08 [SER0198-99, 0242-43]. It used a U.S. telecommunications company (NobelBiz) to provide call routing services for both U.S. and foreign consumers. PX10 ¶127 [ER0488-90]; Dkt. 30 at 10 [SER0074]; Dkt. 26-1 at 10 [SER0272]. It used a U.S. call center, operated by a U.S. company (Infocu5), to field calls from consumers both here and abroad. PX11 ¶14, Att. G at 48 [SER0197, 0228] (discussing overseas products Dermagen IQ and Expert Lift); Dkt. 30-12 Exh. 11 at 6-11 [SER0108-13] (listing products by country). And Hardwire used a U.S. payment network (Processing.com) to facilitate the processing of charges for both domestic and foreign consumers. Dkt. 30 at 14 [SER0078] (noting that Defendants had hundreds of active Processing.com merchant accounts located overseas); Dkt. 53 at 5 [SER0005] (noting that Hardwire used Processing.com to set up accounts to process charges in euros and pounds).

Hardwire's partnership with U.S.-based Triangle Media was—as Hardwire's principal Keer described it—"the core backbone of [Hardwire's] subscription business." PX11 Att. D at 29 [SER0212]. Triangle Media monitored the call centers that handled calls from Hardwire's domestic and international consumers. PX11 ¶14, Att. G at 43-60 [SER0197, 0223-40]. Triangle Media also set up and

managed an extensive network of merchant accounts in the U.S. and abroad to process Hardwire's consumer charges. Dkt. 30 at 12, 14 [SER0076, 0078]; *see also* Dkt. 30-5 Exh. 4 at 2-6 [SER0098-102] (setting up U.S. and U.K. merchant accounts). To protect the scheme from scrutiny, Triangle Media formed hundreds of shell companies, recruiting ordinary people to "front" as merchants to open those accounts. Dkt. 30 at 4, 11-14, 18 n.13 [SER0068, 0075-78, 0084]. As the Receiver determined, the constant creation of these merchant accounts was the "lifeblood" of the enterprise because it allowed Hardwire to continue charging consumers even as banks closed other accounts due to customer complaints. *Id.* at 4, 12 [SER0068, 0076]. Triangle Media monitored the merchant accounts and transferred the money from those accounts to entities controlled by Keer and Hardwire. *Id.* at 12, 15, 20 [SER0076, 0079, 0084]. Hardwire, in turn, then routed funds back to Triangle Media to cover Triangle Media's expenses. *Id.* at 20 [SER0084].

C. The SAFE WEB Act

In the early 2000s, as internet-based commerce began its explosive growth and deceptive practices proliferated online, the FTC grew concerned about foreign scammers preying on United States consumers and about companies using the United States as a hub for international scams. Although the agency had long used the FTC Act to address foreign commerce, *see, e.g.*, *Branch v. FTC*, 141 F.2d 31

(7th Cir. 1944), it proposed to Congress legislation to "address the challenges posed by globalization of fraudulent, deceptive, and unfair practices," and to protect American consumers from "fall[ing] victim to foreign con artists." Fed. Trade Comm'n, *The US SAFE WEB Act: Protecting Consumers from Spam, Spyware, and Fraud – A Legislative Recommendation to Congress* i (2005) ("*Legislative Recommendation*").[4] The FTC also wanted Congress to underscore the agency's ability to "deter[] fraud operators from using the United States as a haven from which they can develop and then export fraudulent schemes." *Legislative Recommendation, An Explanation of the Provisions of the US SAFE WEB Act* at 15.[5]

Congress responded by enacting the FTC's proposed "Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006" ("SAFE WEB Act"), Pub. L. No. 109-455, 120 Stat. 3372 (2006). As pertinent here, the SAFE WEB Act adopted the exact language proposed by the FTC to

[4] Available at https://www.ftc.gov/sites/default/files/documents/reports/us-safe-web-act-protecting-consumers-spam-spyware-and-fraud-legislative-recommendation-congress/ussafeweb.pdf.

[5] Available at https://www.ftc.gov/sites/default/files/documents/reports/us-safe-web-act-protecting-consumers-spam-spyware-and-fraud-legislative-recommendation-congress/explanation-provisions-us-safe-web-act.pdf.

amend Section 5 of the FTC Act,[6] thereby responding to both of the agency's enforcement concerns by clarifying that "the term 'unfair or deceptive acts and practices' includes such acts or practices involving foreign commerce" so long as the acts (1) "cause or are likely to cause reasonably foreseeable injury within the United States," or (2) "involve material conduct occurring within the United States." 15 U.S.C. § 45(a)(4)(A)(i) -(ii). Congress provided further that the FTC could seek "all remedies available" for foreign misconduct, including "restitution to domestic or foreign victims." 15 U.S.C. § 45(a)(4)(B).

The FTC has invoked its authority under the SAFE WEB Act many times to stop fraudulent conduct by foreign defendants operating global schemes targeting both domestic and foreign consumers. Contrary to Hardwire's repeated claim, there is nothing novel about the agency using the Act as it did here. For example, in *FTC v. Willms*, No. 2:11-cv-00828-MJP (W.D. Wash., filed May 16, 2011), the FTC sued an online operation very similar to Hardwire's that deceived consumers in the U.S. and elsewhere (Canada, the United Kingdom, Australia, and New Zealand) by promising "free" or "risk-free" trial products. Most of the defendants were Canadian. The district court preliminarily enjoined the defendants from

[6] *See Legislative Recommendation, Draft US SAFE WEB Act* at 4, available at https://www.ftc.gov/sites/default/files/documents/reports/us-safe-web-act-protecting-consumers-spam-spyware-and-fraud-legislative-recommendation-congress/proposed-us-safe-web-act.pdf.

engaging in their deceptive conduct (or even using negative options) without geographic limitation.[7] In *FTC v. Innovative Marketing, Inc.*, No. 1:08-cv-03233-RDB (D. Md., filed Dec. 2, 2008), the FTC sued to block the defendants, including foreign corporations and individuals, from using "scareware" to trick millions of consumers around the world into buying bogus software. The district court entered a preliminary injunction much like the present one, prohibiting the defendants from engaging in their fraudulent conduct throughout the world, suspending their websites, and freezing all assets—all without geographic limitation.[8]

Likewise, in *FTC v. Atkinson*, 1:08-cv-05666 (N.D. Ill., filed Oct. 6, 2008), the FTC shut down a vast international spam network that peddled bogus prescription drugs, weight-loss pills, and male-enhancement products to U.S. and foreign consumers. As here, the defendants included both U.S. and foreign companies and individuals. The district court enjoined all of them from continuing

[7] *See* Amended Complaint, available at https://www.ftc.gov/sites/default/files/documents/cases/2011/09/110902jwillmscmpt.pdf; Order Granting Preliminary Injunction (adopting FTC's proposed Preliminary Injunction), available at https://www.ftc.gov/sites/default/files/documents/cases/2011/09/110913jwillmspiorder.pdf; Proposed Preliminary Injunction, Dkt. No. 3-1, *FTC v. Willms*, No. 2:11-cv-00828 (W.D. Wash.), available through the court's ECF system.

[8] See Complaint, available at https://www.ftc.gov/sites/default/files/documents/cases/2008/12/081202innovativemrktgcmplt.pdf; Preliminary Injunction, available at https://www.ftc.gov/sites/default/files/documents/cases/2008/12/081215innovativeprelim.pdf.

to engage in fraudulent practices, again without geographic limitation.[9] And in *FTC v. PCCare247 Inc.*, No. 1:12-cv-07189-PAE (S.D.N.Y., filed Sept. 24, 2012), the court enjoined the defendants, mostly based in India, from engaging in deceptive practices involving tech support scams. The court also suspended websites and disconnected phone numbers without any geographic limitation.[10]

D. The FTC's Enforcement Lawsuit And The Preliminary Injunction

On June 25, 2018, the FTC sued Hardwire, Triangle Media, Phillips, and one of the shell corporations seeking a permanent injunction and other equitable relief for violations of the FTC Act, ROSCA, and EFTA. Dkt. 1 ¶1; *id.* at 1 [ER1056-57]. The Court entered a temporary restraining order, and later a preliminary injunction, that enjoined defendants' illegal conduct, froze their assets, and placed the corporate defendants under receivership. Dkt. 11 [ER0364-95]; Dkt. 75 [ER0001-28].

Hardwire refused to provide information about its business operations to the Receiver, as required by the TRO (prompting the Receiver to file a contempt

---

[9] See Complaint, available at https://www.ftc.gov/sites/default/files/documents/cases/2008/10/081014atkinsoncmpt.pdf; Permanent Injunction, available at https://www.ftc.gov/sites/default/files/documents/cases/2009/11/091130atkinsjudgement.pdf.

[10] *See* Complaint, available at https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121003pccarecmpt.pdf; Preliminary Injunction, Dkt. No. 65, *FTC v. PCCare 247 Inc.*, No. 1:12-cv-07189-PAE (S.D.N.Y. Nov. 16, 2012), available through the court's ECF system.

motion). Dkt. 33-1 at 2-5 [SER0051-54]. It asked the court to modify the TRO to allow it to reactivate the U.S. telephone lines it used for foreign calls, claiming that deactivation would cripple its overseas business. Dkt. 26-1 at 4-5 [SER0266-67]. It also asserted that it should be permitted to continue marketing its alleged "risk free" trials to foreign consumers. *Id.* at 5 [SER0267]. The district court declined to modify the TRO. It found that the FTC was likely to succeed in showing that "Hardwire's foreign conduct causes or is likely to cause reasonably foreseeable injury within the United States"—which by itself was enough to reach Hardwire's foreign conduct. Dkt. 31 at 4 [SER0063]. The court also found that the FTC was "likely to succeed on the merits of its claim that Hardwire's foreign commerce involves material conduct occurring within the United States." *Id*.

On August 24, 2018, after briefing and a hearing, the district court entered a preliminary injunction, explaining its reasoning in a painstaking 30-page Memorandum Order. As the court noted, Hardwire and its co-defendants did not challenge the FTC's likelihood of success on the merits of the causes of action in the complaint. Dkt. 74 at 10 [ER0038]. Nor did Hardwire oppose the issuance of a preliminary injunction with respect to its conduct within the United States. Dkt. 74 at 17 [ER0045]. Hardwire sought only "to prevent the Court from issuing an order enjoining its foreign operations." *Id*. at 17 [ER0045].

Hardwire argued that its foreign operations—its foreign websites selling to foreign consumers—were "entirely separate and distinct from its U.S. operations" and therefore did not fall within the reach of the FTC Act. Dkt. 36 at 19 [ER0263]. The district court rejected that claim on two grounds. Dkt. 74 at 18-19 [ER0045-47]. First, it found that evidence presented by the FTC and the Receiver (who had provided a detailed 26-page report as well as legal memoranda) showed that Hardwire relied extensively on U.S.-based companies and services—including a call center, a payment gateway, a payment network, and marketing operations—with respect to *both* its U.S. *and* foreign sales. Indeed, as the Receiver reported, just one month before the TRO was entered, Hardwire, through a U.S payment network, filed "dozens" of foreign merchant account applications to process consumer charges in U.S. dollars. *Id*. at 19 [ER0047]; Dkt. 53 at 4 [SER0004]. The district court found "a likelihood that Hardwire's foreign conduct involves material conduct occurring within the United States and is also reasonably likely to cause or has caused reasonably foreseeable injury in the United States." Dkt. 74 at 19-20 [ER0047-48]. Hardwire's foreign conduct therefore fell within the reach of the FTC Act by virtue of the SAFE WEB Act amendments.

Second, the court also found that the FTC was likely to succeed in proving that Hardwire and its U.S.-based co-defendants operated as a common enterprise. *Id*. at 20 [ER0048]. Citing the Receiver's report, the court found that the

companies "were controlled by the same primary parties, shared employees and resources, commingled corporate funds, and appear to transact business through a maze of interrelated companies." *Id*. at 24 [ER0052]. "The few distinctions between the companies … [were] superficial in nature in comparison to the overwhelming evidence of the companies' interrelated functions." *Id*. For example, as the Receiver explained, "the use of a Los Angeles company to file Bulgarian merchant applications to process in U.S. dollars, while at the same time filing numerous other applications on behalf of Hardwire seeking to process in euros and pounds, demonstrates that Hardwire's operation was not run as separate U.S. and international operations, but instead is one unified operation with significant roots in this country." *Id.* (quoting Dkt. 53 at 5 [SER0005]). The likelihood that the companies acted as a single concerted enterprise provided an "additional basis" to find that the FTC Act applied to Hardwire's foreign operations. Dkt. 74 at 25 [ER0053].

The district court found that applying a preliminary injunction to Hardwire's foreign business conduct was in the "public interest" because it would protect consumers from unlawful and deceptive conduct. *Id*. And it found that a continued freeze of Hardwire's foreign assets was warranted to preserve funds for restitution, noting Hardwire's practice of moving "funds throughout the world" and the disparity between the value of the frozen assets (approximately $1.8 million) and

the tens of millions of dollars of estimated consumer harm. *Id*. at 25-26 [ER0053-54].

SUMMARY OF ARGUMENT

The SAFE WEB Act authorizes the FTC to stop deceptive foreign practices if those practices 1) "cause or are likely to cause reasonably foreseeable injury within the United States" or 2) "involve material conduct occurring within the United States." 15 U.S.C. § 45(a)(4)(A)(i)-(ii). Congress added those provisions to enable the FTC to combat fraudulent practices worldwide, so long as the statutory conditions are met. The district court found as a factual matter that the FTC was likely to show that Hardwire's foreign fraudulent practices satisfied both of the SAFE WEB Act predicates, warranting a preliminary injunction halting its global deceptive marketing scheme. Hardwire's effort to portray this decision as legal error is meritless. Substantial evidence—which Hardwire's brief wholly ignores—showed that Hardwire's foreign operations were deeply rooted in the United States, intertwined with its domestic activities, and likely to cause forseeable injury to U.S. consumers. Its activities were of the very type that Congress enacted the SAFE WEB Act to reach.

1. The district court properly exercised its discretion when it enjoined Hardwire's fraudulent activity worldwide and rejected Hardwire's bid to continue defrauding foreign consumers. The evidence showed that Triangle Media, a U.S

company, was a central component—as Hardwire's owner described it, the "backbone"—of the Hardwire scheme. Indeed, as the district court found, the two companies were so intertwined that they effectively operated as a single-entity "common enterprise." Hardwire's entire case rests on the idea that there are separate "domestic" and "foreign" operations that can be meaningfully separated, but there were no such separate operations. Rather, as the district court found—and Hardwire does not challenge—the U.S. and foreign businesses were one and the same enterprise.

Beyond its common operation with Triangle Media, moreover, Hardwire directly used a multitude of U.S. companies and U.S. facilities to carry out both the domestic and foreign aspects of its scheme, making the United States the core base for its global fraudulent operations. Overseas, the evidence showed, Hardwire used its network of foreign accounts and false merchant "fronts" to carry out fraudulent transactions with U.S. consumers. The overwhelming record leaves no room for doubt that the district court properly enjoined Hardwire's foreign operations because they involved material conduct occurring in the United States and posed a foreseeable risk of harm to American consumers.

That record, which Hardwire barely mentions and does not refute, fatally undercuts the claim that the FTC Act does not reach Hardwire's foreign operations. In particular, the claim that its foreign and domestic operations were entirely

separate is false and squarely collides with considerable evidence showing that the operations were intertwined, that the foreign operations depended on U.S. services and facilities, and that U.S. consumers were likely to be targeted by foreign operations.

Hardwire's attempt to portray its U.S. operations as a *de minimis* part of its business is therefore irrelevant. Even if the account were accurate, the relative volume of domestic sales does not undermine Hardwire's substantial conduct in this country supporting its foreign sales. In any event, the 7 percent figure Hardwire touts rests on a cherrypicked sales figure from a single month.

F. Hoffmann-La Roche Ltd. v. Empagran S.A., 542 U.S. 155 (2004), on which Hardwire relies heavily, has no application here. The statute at issue in *Empagran* was intended to restrict the extraterritorial application of U.S. antitrust law and thus set a high bar for doing so. The SAFE WEB Act, by contrast, was specifically meant to *extend* the reach of the FTC Act to encompass deceptive foreign practices and thus set a permissive test. The Supreme Court's interpretation of the reach of the antitrust law thus sheds no light on the SAFE WEB Act.

2. Hardwire's claim that the district court erred by granting preliminary injunctive relief that exceeds the scope of permissible final relief is meritless. The contention merely rehashes Hardwire's argument that its foreign fraudulent practices are beyond the reach of the FTC Act, and it fails for all the same reasons.

Nor was the district court disabled from enjoining Hardwire's operations throughout the globe by Hardwire's litigation-inspired pledge to sever its U.S. connections and stop victimizing U.S. consumers. Hardwire's domestic and foreign operations have been intertwined for years, and the district court was not stripped of its power to enforce U.S. law reaching all of Hardwire's business by an empty pledge that Hardwire would conduct its business differently in the future. For one thing, Hardwire—a serial fraudster—could surreptitiously resume its domestic activities later. For another, a promise to change business practices going forward does not undo Hardwire's irreversible foundation in the United States: its entire scheme was conceived, developed, and perfected using U.S. facilities and in conjunction with an integrally related U.S. company and its U.S.-resident owner. The broad terms of the SAFE WEB Act confer upon the district court authority to reach all of Hardwire's fraudulent activities anywhere.

Hardwire's related argument that that the district court could have provided complete relief with a less restrictive injunction also fails. The court considered a less restrictive injunction and decided it would be insufficiently protective. Hardwire shows no clear error in that quintessential exercise of judicial judgment.

STANDARD OF REVIEW

A district court order granting a preliminary injunction is reviewed for abuse of discretion. *Johnson v. Couturier*, 572 F.3d 1067, 1078 (9th Cir. 2009). That

standard is "limited and deferential"; this Court "may only reverse the district court's decision if it was based on an erroneous legal standard or clearly erroneous findings of fact." *Conservation Cong. v. U.S. Forest Serv.*, 720 F.3d 1048, 1053 (9th Cir. 2013); *see also FTC v. Affordable Media, LLC*, 179 F.3d 1228, 1233 (9th Cir. 1999). If the district court "applied the correct legal rule to the relief requested," the district court's decision must be upheld unless it "resulted from a factual finding that was illogical, implausible, or without support in inferences that may be drawn from the facts in the record." *M.R. v. Dreyfus*, 697 F.3d 706, 725 (9th Cir. 2012) (cleaned up).

ARGUMENT

Hardwire concedes that the FTC is likely to show that its activities were fraudulent and that the district court properly enjoined its unlawful domestic conduct, froze its assets, and appointed a receiver. The narrow issue presented is whether the court was required to allow Hardwire to continue deceiving foreign consumers in the meantime. As we show below, the record firmly supports the district court's determinations that the Hardwire scheme, which harmed U.S. consumers, was unified and indivisible, and that the frauds perpetrated abroad involved material conduct within the United States. All of Hardwire's unlawful activities across the globe therefore fell within the scope of the SAFE WEB Act, and the district court properly enjoined them.

I. THE DISTRICT COURT PROPERLY ENJOINED ALL OF HARDWIRE'S FRAUDULENT PRACTICES, FOREIGN AND DOMESTIC

Congress expressly granted the FTC authority to take action against deceptive acts or practices "involving foreign commerce" when either of two conditions is met: 1) the unlawful actions "cause or are likely to cause reasonably foreseeable injury within the United States"; or 2) they "involve material conduct occurring within the United States." 15 U.S.C. § 45(a)(4)(A)(i)-(ii).[11] In such cases, the FTC may seek "all remedies available . . . including restitution to domestic or foreign victims." 15 U.S.C. § 45(a)(4)(B). Hardwire attempts to paint this case as a novel matter of first impression (it is not, as explained on pages 12-14 above), but in reality this case involves the straightforward application of the plain terms of a statute whose meaning is not in dispute.

The district court found as a matter of fact that the FTC is likely to show both that Hardwire's foreign fraudulent practices harmed or were likely to harm U.S. consumers and that they involved material domestic conduct. The record firmly supports those conclusions, and Hardwire has shown no error in them at all,

[11] The extraterritorial reach of ROSCA and EFTA is coextensive with that of Section 5. *See* 15 U.S.C. § 8404(a) (the FTC enforces ROSCA "with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act … were incorporated into and made a part of" ROSCA); 15 U.S.C. § 1693o(c) (a violation of EFTA is "deemed a violation of a requirement imposed under th[e] [FTC] Act").

let alone clear error. Indeed, Hardwire ignores the court's extensive factual findings.

A. The District Court Correctly Found That Hardwire's Foreign Business Operations Likely Involved Material Domestic Conduct And Were Likely To Harm U.S. Consumers

As the district court determined, a central component of the Hardwire scheme is a U.S. company with U.S. offices, U.S. ownership, and U.S. employees. That situation is sufficient by itself to support a finding that Hardwire's deceptive acts or practices in foreign commerce likely involved material conduct in the U.S. The two principal corporations at the heart of the scheme are Hardwire and Triangle Media, which Keer, Hardwire's principal owner, described as "the core backbone of [Hardwire's] subscription business" and its "most important business relationship." PX11 Att. D at 29 [SER0212]. Triangle Media is incorporated and based in the U.S.; its owner, Brian Phillips, is a U.S. resident. Dkt. 48 ¶¶6, 9 [SER0034]. Phillips also has held ownership interests and corporate roles in Hardwire. Dkt. 30 at 18, 21 [SER0082, 0085].

The record bears out Keer's description. Triangle Media materially supported Hardwire's foreign and domestic fraud. Its employees monitored call centers that handled calls from both domestic and foreign consumers. PX11 ¶14, Att. G at 43-60 [SER0197, 0223-40]. Triangle Media also provided a payment gateway, Tripayments, to charge both domestic and foreign consumers. Dkt. 74 at

18 [ER0046]; Dkt. 36 at 7, 13 [ER0251, ER0257]; Dkt. 30 at 24-25 [SER0088-89]. Triangle Media's principal, U.S. resident Phillips, facilitated the submission of merchant account applications for domestic and foreign applicants. Dkt. 30-5 Exh. at 4-5 [SER0100-01] (Phillips setting up U.K. merchant account). His laptop contained hundreds of completed merchant account application packages for people across the globe going back to at least 2011. Dkt. 30 at 14 [SER0078]. Triangle Media also tracked Hardwire's sales both in the US and abroad. PX11 ¶8, Att. A at 21 [SER0195, 0210].

That evidence shows by itself that the global operation of the Hardwire scheme involved material conduct occurring in the United States. But the links between Hardwire and U.S.-based Triangle Media went beyond a mere business arrangement. The district court found that the two companies were so intertwined that they effectively operated as one-and-the-same entity—a common enterprise. They were:

> controlled by the same primary parties, shared employees and resources, commingled corporate funds, and appear to transact business through a maze of interrelated companies. . . . The few distinctions between the companies – the fact that they maintained separate bank accounts, for instance – are superficial in nature in comparison to the overwhelming evidence of the companies' interrelated functions.

Dkt. 74 at 24 [ER0052]. Because common enterprise companies do not operate as genuinely separate entities, they "may be held liable for the deceptive acts and

practices of the others" in the enterprise. *FTC v. Grant Connect, LLC*, 763 F.3d 1094, 1105 (9th Cir. 2014).

The district court's factual finding of common enterprise—which Hardwire does not challenge—leads inevitably to the conclusion that Hardwire's foreign conduct had (and will continue to have) material contacts with the United States.[12] There are no separate domestic and foreign operations.

Beyond the common enterprise, moreover, the district court found, with definitive record support, that Hardwire directly engaged in material domestic conduct contributing to the fraud. Dkt. 74 at 17-19 [ER0045-48]. These activities were of the very type that spurred the FTC to recommend to Congress that it enact the SAFE WEB Act to prevent the United States from becoming a haven for foreign fraud. Hardwire used Processing.com, a U.S. company, to set up hundreds of domestic and foreign merchant accounts to process domestic and foreign consumer charges. Dkt. 74 at 19 [ER0047] (discussing dozens of foreign merchant accounts filed through Processing.com in the month before the TRO); Dkt. 30 at 14 [SER0078] (defendants had hundreds of active Processing.com merchant accounts

[12] The court found that the common enterprise survived the realignment of the companies in the Fall of 2017. A contemporaneous email, for example, described the realignment as "a change in corporate structure [that] really is mostly a formality" that would not affect the companies' day-to-day operations. Dkt. 74 at 22 [ER0050]; PX11 Att. D at 29 [SER0212]. The court also noted that, as late as March 2018, Hardwire's general manager was still acting on behalf of both companies. Dkt. 74 at 24 [ER0052]; Dkt. 30 at 21 [SER0085].

located overseas); Dkt. 53 at 4-5 [SER0004-05] (Hardwire used Processing.com to set up accounts to process charges in euros and pounds). That conduct was material because the merchant accounts allowed the defendants to process consumer charges and keep a constant stream of income even as other accounts were closed for high levels of refunds and chargebacks. Dkt. 30 at 4, 11-12 [SER0068, 0075-76].

Beyond that, Hardwire used a U.S-based domain registrar, Wild West Domains, to register hundreds of domain names, including for foreign websites and Hardwire's own website, hardwireinteractive.com. Dkt. 31 at 4 [SER0063];[13] PX10 ¶132 [ER0491-93];[14] PX11 ¶19 [SER0200]. These websites were then hosted on servers of U.S. provider Amazon Technologies. Dkt. 31 at 4 [SER0063]; PX11 ¶21 [SER0200]. Hardwire also used a U.S.-based online marketing network, Clickbooth.com, to advertise its U.S. and foreign websites to consumers in the U.S.

[13] The district court noted that its prior order denying Hardwire's motion to modify the TRO provided additional reasons to support its findings. *See* Dkt. 74 at 20 n.2 [ER0048].

[14] Some of the listed websites can readily be identified as foreign-facing because their domain names end in, for example, ".co.uk" or ".fr." *See* PX10 at 527, 538 [ER0806-07, 0817]. However, many of the foreign webpages were actually subpages of websites with a ".com" domain. *See e.g.*, PX11 ¶¶24, 30, 34 [SER0202, 0204, 0205]. For example, the U.S. and U.K. webpages for skin creams Erase/Repair HA and Dermagen IQ, respectively, are part of the www.findbeautyandtruth.com domain, which was registered by Wild West Domains. PX10 ¶¶64, 132a [ER0465, 0491]; PX11 ¶ 23 [SER0201].

and abroad. Dkt. 74 at 18 [ER0046]; PX11 ¶17, Att. J at 107-08 [SER0198-99, 0242-43].

In addition, Hardwire used a U.S. telecommunications company, NobelBiz, for all of its telecom and call routing services for both U.S. and foreign consumers. Dkt. 31 at 4 [SER0063]; Dkt. 30 at 10 [SER0074]; PX10 ¶127 [ER0488-90]; Dkt. 26-1 at 10 [SER0272]. Hardwire effectively admitted that the U.S.-based call routing function was an essential part of its foreign transactions: after the Receiver instructed NobelBiz to deactivate Hardwire's telephone lines, Hardwire sought to modify the TRO on the ground that deactivation would cripple its overseas business. Dkt. 26-1 at 4 [SER0266]. Hardwire also used a U.S. call center, operated by U.S. company Infocu5, to field calls from customers here and abroad. Dkt. 74 at 18 [ER0046]; PX11 ¶14 [SER0197]; PX11 Att. G at 48 [SER0228] (discussing overseas products Dermagen IQ and Expert Lift); Dkt. 30-12 Exh. 11 at 6-11 [SER0108-13] (listing products by country).[15] In these instances, Hardwire did not maintain separate accounts for its domestic and foreign operations. Rather, it maintained single, unitary accounts with its U.S. service providers for all of its

[15] Hardwire craftily claimed below that it "never used any customer service personnel located inside the U.S. to serve foreign-language speaking customers outside the U.S." Dkt. 36 at 13-14 [ER0257-58] (citing Dkt. 36-1 ¶11 [ER0241-42]). Tellingly, however, it did not contend that it never used U.S. call centers for calls from foreign English-speaking customers, such as those in the UK or Australia.

operations, both foreign and domestic. *See, e.g.*, PX10 ¶132 [ER0491-93]; PX11 Att. J at 107-08 [SER0242-43]. Furthermore, Hardwire itself had at least two employees or contractors in the U.S acting on its behalf until the TRO took effect. Dkt. 53 at 6-7 [SER0006-07]. Hardwire's general manager was stationed in San Diego for most of 2017. Dkt. 74 at 24 [ER0052]; Dkt. 30 at 21 [SER0085].

In addition to the overwhelming amount of material domestic conduct, the court also properly found a reasonable probability that the scheme would continue to injure U.S. consumers through its foreign operations. Dkt. 74 at 19-20 [ER0047-48]. Roughly half of Hardwire's 208 active foreign merchant accounts on Processing.com have the ability to transact in U.S. dollars. Dkt. 30 at 14 [SER0078]. Only one month before the TRO, Hardwire continued to register foreign merchant accounts seeking to do business in the U.S. For example, on May 29, 2018, Hardwire used a Bulgarian citizen to apply for a merchant account stating an intent to process up to 100,000 U.S. dollars per month doing business through U.S. toll free numbers. Dkt. 74 at 19 [ER0047]; Dkt. 53 at 4 [SER0004]; Dkt. 53-2 at 4-9 [SER0014-19]. Another Bulgarian front company recently applied for an account to process sales of 600,000 U.S. dollars per year, listing a U.S. toll free number, and specifying that it wanted to receive services in the U.S. Dkt. 74 at 19 [ER0047]; Dkt. 53 at 4 [SER0004]; Dkt. 53-3 at 3, 5 [SER0024, 0026]; *see also*

Dkt. 30-12 Exh. 11 at 23-24, 30-36, 70-71 [SER0125-26, SER0132-38, SER0172-73] (showing various foreign shell companies selling products in U.S. dollars).

The record leaves no room for doubt that the district court properly enjoined Hardwire's foreign transactions because they involved material conduct occurring in the United States and posed harm to American consumers.

B. Hardwire Fails To Refute The Substantial Evidence Of Material Domestic Conduct

Hardwire agrees that the FTC Act reaches foreign activities that involve material domestic conduct; indeed, throughout its brief it recites the statute saying so directly. Br. 1, 12, 22, 29, 37, 44, 47. Yet Hardwire fails to grapple with the substantial evidence that its foreign operations involved material conduct in the United States. Its brief ignores the record and the district court's findings entirely. In particular, it does not contest the district court's finding that Hardwire and Triangle Media operated as a common enterprise, which by itself defeats its claim that the district court failed to "consider[] whether the overseas-based transactions that it was enjoining fell within the scope of its equitable authority under the Safe Web Act." Br. 23. The district court plainly considered that question and answered definitively that all of Hardwire's conduct falls within the scope of the statute.

Instead, Hardwire attempts to sidestep the implications of its deeply rooted U.S. conduct and corporate relationships by claiming that the Court should examine only the specifics of individual transactions. Thus, it asserts that the sale

of goods in a foreign country to foreigners does not "involve[] the United States in any way," Br. 2, and that its "advertising and sales practices outside of the United States were entirely separate and materially different" from its domestic practices. Br. 8. It claims similarly that the preliminary injunction "indiscriminately" enjoins "transactions in foreign commerce that have no connection to or effect on United States commerce," Br. 16, and describes its foreign practices as "wholly international operations." Br. 19; *see also id*. at 28.

Those descriptions founder on the record in two fundamental ways. First, as the evidence before the district court demonstrated, even the sale on a U.K. website to a British consumer could involve U.S.-based web domains registered by a U.S. company; telephone numbers assigned, routed, and staffed by U.S.-based companies; and payments processed through a U.S.-based payment network on accounts arranged for by a U.S. resident. Such transactions obviously involve material conduct in the United States and are solidly within the scope of behavior Congress meant the FTC to target when it enacted the SAFE WEB Act.

Second, as the district court also recognized, examining Hardwire's conduct transaction-by-transaction ignores the reality that Hardwire's foreign operation is integrally intertwined with its U.S. operation. Hardwire's conduct is not merely a series of individual transactions, but a complex, global scheme involving executive direction, shell corporations, back-office operations, and related support systems,

the "backbone" of which is located in the U.S., no matter where a given transaction takes place. Defendants used the same U.S.-based payment network, online marketer, telecommunications provider, domain registrar, web host, and call center for foreign and domestic sales alike. *See supra* pp. 8-9.[16] The same staff worked on foreign and domestic aspects of the fraud concurrently with no separation between foreign and domestic business. *See, e.g.*, Dkt. 30-5 Exh. 4 at 4-6 [SER0100-02] (email setting up both foreign and domestic merchant accounts).[17]

The district court thus correctly rejected Hardwire's assertion that its international operations are "entirely separate and distinct from its U.S. operations." Dkt. 74 at 18 [ER0046]. Relying on the Receiver's findings, the court concluded that the evidence "demonstrates that Hardwire's operation was not run as separate U.S. and international operations, but instead is one unified operation

[16] Hardwire asserts that "foreign websites selling Hardwire products to foreign consumers were designed, owned, and operated by entities located outside of the United States." Br. 9. The reference to foreign "entities" appears to be a reference to Hardwire itself. *See* Dkt. 36 at 14 [ER0258] (suggesting that Hardwire designs, develops, implements, and publishes marketing for its products outside the US); PX10 Att. R at 516-42 [ER0795-821] (listing Hardwire as owner of hundreds of websites, including foreign ones). But as the district court found, there is no meaningful distinction between Hardwire and U.S.-based Triangle Media (and Hardwire does not contest this factual finding on appeal).

[17] Hardwire's assertion that its advertising and sales practices in the U.S. and abroad were "entirely separate and materially different" is supported solely by the declaration of its principal, Keer. Br. 8 (citing Dkt. 36-1 ¶2 [ER0240]). Keer's conclusory recitation cannot be squared with the record, and in any event cannot by itself demonstrate a clear error in the district court's fact-finding.

with significant roots in this country." Dkt. 74 at 19 [ER0047] (quoting Dkt. 53 at 5 [SER0005]).

Hardwire also appears to claim that the preliminary injunction is somehow inappropriate because the complaint "failed to provide … any evidence concerning what (if any) injuries were allegedly suffered by foreign consumers." Br. 23; *see also id.* at 40-41. For all the reasons above, the preliminary injunction is fully justified by the evidence submitted showing material conduct within the United States. And, the complaint provided ample notice that Hardwire's overseas acts were within the scope of the complaint and subject to relief, including injunction. The allegations are not limited in geographic scope either in the description of the unfair or deceptive practices or in the allegation of consumer injury. *See* Dkt. 1 ¶¶38-49, 55-56, 61-65 [ER1072-79]. The complaint's allegations of consumer harm apply equally to U.S. and foreign consumers, who were subject to the same deceptive conduct the complaint describes. In light of that record, the absence of specific allegations of harm to foreign consumers is immaterial. In any event, discovery has not yet even begun, and the FTC may amend its complaint as necessary after it gains more evidence.

Hardwire's attempt to portray its U.S. operations as a *de minimis* part of its business representing only 7 percent of its revenue fails. Br. 2, 8, 22. For starters, no matter what Hardwire's U.S. sales are, they do not erase the very substantial

material conduct that took place domestically. Moreover, the 7 percent figure is misleading. Hardwire's net sales in the U.S. in 2017 were approximately $46 million, compared with £16 million in the UK and €27 million in the EU. Dkt. 30 at 24 [SER0088]. In the first half of 2018, U.S. sales were $12 million, compared with £16 million in the UK and €16 million in the EU. *Id.* at 24-25 [SER0088-89]. The 7 percent figure appears to come from one month's revenue in June 2018. Dkt. 26-2 ¶5 [ER0313]. Nor does the record show that Hardwire intended to withdraw from the U.S. market. *See* Br. 8. Keer anticipated growth in U.S. sales as high as 100 percent in 2017. Dkt. 30 at 23 [SER0087]; Dkt. 30-27 Exh. 26 at 4 [SER0187]. His expectations were dashed, and U.S. revenue declined, because banks began to shut down Hardwire's U.S. merchant accounts beginning in late-2017. Dkt. 30 at 23-24 [SER0087-88]; Dkt. 53 at 4 [SER0005]. As mentioned above, Hardwire continued to register new merchant accounts seeking to do hundreds of thousands of dollars in U.S. business until a month before the TRO. *See supra* p. 29.

Finally, Hardwire gets no help from the Supreme Court's decision in *F. Hoffmann-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155 (2004). Hardwire reads *Empagran* as holding that when unlawful conduct "affects both entities outside and within the United States, but the adverse foreign effect is independent of any adverse domestic effect, [U.S.] law did not apply" to the foreign conduct. Br. 24. It contends that the district court erred by failing to determine whether the domestic

injury was independent of the foreign injury. Br. 23-24. *Empagran* establishes no such error.

Empagran interpreted a statute that implements a far more restrictive standard for extraterritorial application than the SAFE WEB Act. The case involved an international conspiracy among vitamin manufacturers to fix prices in violation of the Sherman Act. Among the plaintiffs were foreign companies that purchased vitamins outside of the United States at inflated prices. The district court's jurisdiction over the foreign companies' claims was governed by the Foreign Trade Antitrust Improvements Act ("FTAIA"), which prohibits the application of the Sherman Act to conduct involving foreign trade or commerce unless such conduct "has a direct, substantial, and reasonably foreseeable effect" on domestic commerce. 15 U.S.C. § 6a; *see also* 15 U.S.C. § 45(a)(4)(A) (incorporating same standard for antitrust cases brought under the FTC Act). The Court concluded that foreign transactions that caused foreign injury independent of any domestic effect did not meet that test.

The holding has no applicability here because the SAFE WEB Act is fundamentally different from the FTAIA. Congress intended the FTAIA to *restrict* the extraterritorial application of U.S. antitrust laws. *See Empagran*, 542 U.S. at 161. The SAFE WEB Act, by contrast, was specifically meant to *extend* the reach of the consumer protection law to encompass deceptive foreign practices so long as

they involve material domestic conduct; indeed, Congress specified that the FTC could secure relief for defrauded foreign victims. In keeping with the legislative intent, the SAFE WEB Act standard is far more permissive than the FTAIA's restrictive approach. Because the SAFE WEB Act applies when there is foreign harm rooted in material U.S. conduct, the district court did not need to address whether foreign injury was independent of domestic effects.[18]

II. THE DISTRICT COURT PROPERLY EXERCISED ITS DISCRETION IN DETERMINING THE SCOPE OF PRELIMINARY INJUNCTIVE RELIEF

Hardwire further argues that the district court erred by granting preliminary injunctive relief that exceeds the scope of permissible final relief and by failing to consider a less restrictive alternative. The claims boil down to a rehash of Hardwire's argument that its foreign fraudulent practices are beyond the reach of the FTC Act—and they fail for all the reasons stated above. Hardwire's cramped view of the district court's equitable powers is meritless.

[18] *Empagran* also distinguished between private suits and government suits and suggested that the government had broader authority even under the FTAIA to protect injured foreign consumers. The Court noted that "once the Government has successfully borne the considerable burden of establishing a violation of law, all doubts as to the remedy are to be resolved in its favor." *Empagran*, 542 U.S. at 170-71 (quoting *United States v. E.I. du Pont de Nemours & Co.*, 366 U.S. 316, 334 (1961)).

A. The District Court Could Properly Enjoin Hardwire's Foreign Fraudulent Practices Notwithstanding The Promise To Sever U.S. Connections

Hardwire's claim fails at the outset because, for all the reasons discussed above, the injunction entered by the district court does not "exceed[] the scope of the final relief that it has the authority to order after a trial on the merits." Br. 38. As we have explained, the SAFE WEB Act by its plain terms covers the entirety of Hardwire's scheme.

The court's authority was not restricted by Hardwire's pledge that "going forward" it will cease targeting U.S. consumers, abandon its U.S. connections, and restrict its fraudulent business to other countries. Br. 15. As we have shown above, Hardwire's foreign fraud has been intimately intertwined with its domestic business to the degree that there is no meaningful distinction between them. In that situation, forswearing domestic fraud and domestic connections does not deprive the court of its power over the integrated foreign operations. Having determined that the foreign and domestic elements of the fraudulent scheme are unitary and intertwined, the district court had no obligation to disentangle those elements to enable Hardwire to continue its fraud overseas.

Relatedly, Hardwire's promise (Br. 15) to use only "non-United States vendors" going forward cannot magically erase the fact that the entire scheme was conceived, developed, and perfected using U.S. facilities and in conjunction with

an integrally related U.S. company and its U.S.-resident owner. At this point, merely switching service providers does not eliminate Hardwire's irreversible connections to the United States. Indeed, the "lifeblood" of the scheme—the network of hundreds of merchant accounts opened by shell companies throughout the world—was created under the direction of a U.S. resident through a U.S. payment network in furtherance of a U.S.-rooted common enterprise. *See* Dkt. 30 at 4, 12, 14 [SER0068, 0076, 0078]; Dkt. 53 at 4-5 [SER0004-05]; Dkt. 30-5 Exh. 4 at 2-6 [SER0098-102]. Using a new web host or telecommunications provider will not render the Hardwire operation purely foreign because its whole foundation rests on contacts with the United States. Under the broad terms of the SAFE WEB Act, the district court's authority reaches all corporate infrastructure, websites, merchant accounts, contracts, and other assets, means, or instrumentalities that Hardwire developed as part of this U.S.-based illegal scheme.

Moreover, it is "well settled" that voluntary cessation of unlawful conduct does not eliminate the need for injunctive relief, "since otherwise the defendants would be free to return to their old ways." *FTC v. Affordable Media, LLC*, 179 F.3d 1228, 1238 (9th Cir. 1999) (cleaned up); *see United States v. Oregon State Med. Soc.*, 343 U.S. 326, 333 (1952) ("It is the duty of the courts to beware of efforts to defeat injunctive relief by protestations of repentance and reform, especially when abandonment seems timed to anticipate suit, and there is

probability of resumption."). Hardwire took steps to secure credit card processing in U.S. dollars just weeks before the FTC filed this case, *see supra* p. 29, and it continued to rely on U.S. businesses to carry out its fraud until the TRO.[19] Its assurance—spurred only by this litigation—that it will sever its U.S. connections and refrain from victimizing U.S. consumers, if only it can resume its fraudulent practices overseas, is exactly the type of hollow promise that decisions like *Oregon State* and *Affordable Media* warn against.

The district court had good reason to be concerned that Hardwire could continue to cause injury to U.S. consumers through its foreign operations. The entanglement of Hardwire's U.S. and international operations, its rampant use of shell corporations and false merchant "fronts" to avoid detection, and—of particular note—its use of foreign merchant accounts to charge U.S. consumers (PX11 ¶22 [SER0201]) amply justify a preliminary injunction that extends to Hardwire's foreign operations. "[T]hose caught violating the FTC Act must expect

[19] *See* PX11 ¶18, Att. J at 107 [SER0199, 0242] (use of Clickbooth in June 2018); Dkt. 53-2 at 4-5, 9 [SER0014-15, 0019] (use of Processing.com in May 2018); Dkt. 53-3 at 3-4, 10 [SER0024-25, 0031] (same); Dkt. 26-1 at 4 [SER0266] (use of NobelBiz until TRO); PX11 Att. G at 45-46 [SER0225-26] (use of Infocu5 in May 2018); PX11 Att. G at 59-60 [SER0239-40] (use of Triangle Media in June, 2018 for call center monitoring); PX11 Att. E at 33 [SER0216] (June 2018 request for new agreements for Triangle Media's payment gateway); PX11 ¶3 [SER0193-94] (payments of hundreds of thousands of dollars per month to Triangle Media through June 2018).

some fencing in." *Grant Connect*, 763 F.3d at 1105 (quoting *FTC v. Nat'l Lead Co.*, 352 U.S. 419, 431 (1957)) (quotation marks omitted).

Hardwire mistakenly relies on *SEC v. International Swiss Investments Corp.*, 895 F.2d 1272 (9th Cir. 1990), for the argument that a court "may not enjoin Hardwire's future non-United States conduct, nor freeze its foreign assets generated from" those activities. Br. 42. That decision affirmed a district court's broad equitable powers to freeze the assets of a party subject to its jurisdiction—"whether the property be within or without the United States." *Id*. at 1276 (quoting *United States v. First Nat'l City Bank*, 379 U.S. 378, 384 (1965)). But the Court did not address the question of enjoining future overseas conduct or freezing "future assets" derived from that conduct.[20] And for all the reasons discussed, there is no meaningful distinction between Hardwire's United States and non-United States conduct.

B. The District Court Properly Considered Less Restrictive Alternatives

Hardwire finally argues that the district court could have provided complete relief with a less restrictive injunction. In fact, the court considered whether a less restrictive injunction was warranted and decided it would be insufficiently protective. Hardwire shows no clear error in that assessment.

[20] Hardwire seeks a carve-out from the injunction for "future assets." Br. 21, 42. Because the business is shut down, however, there will be no "future assets"—unless Hardwire continues to make sales in violation of the preliminary injunction.

Specifically, the court instructed the Receiver to determine whether any component of defendants' business operations could continue to operate lawfully and profitably and therefore be released from the receivership. Dkt. 11 at 22 [ER0385] (TRO Section XVI, Paragraph S). The answer, the Receiver reported, was no. Dkt. 30 at 3 [SER0067]. The Receiver noted that Hardwire makes some legitimate sales—*i.e.*, sales not involving a "free trial" or negative option feature—through Amazon, but its revenues from these "straight sales" were insignificant. Dkt. 30 at 3 n.1, 9 [SER0067, SER0073]. Indeed, Hardwire did not ask the district court to allow it to continue those sales.

The evidence showed that all of Hardwire's other business operations were intertwined with and inseparable from its domestic fraud and thus properly enjoined. *See supra* pp. 31-33. Moreover, allowing Hardwire to continue to use the same websites and shell companies and contracts to perpetrate its fraud overseas would not address the harm to foreign consumers, whose interests the FTC may also seek to protect under the SAFE WEB Act. *See* pp. 10-12, *supra*. Contrary to Hardwire's contention, U.S. consumers are not the only ones whose interests are at stake.

Hardwire's fox-guarding-the-henhouse argument (Br. at 45) that the extraterritorial application of the preliminary injunction "actually compromises" the FTC's consumer protection goals is ludicrous. Although Hardwire claims that

the injunction "depriv[es] foreign consumers of vital customer support and refund services," *id.*, many consumers contacted customer service in the first place precisely because they were being charged for products and continuity programs that they never ordered—and Hardwire resisted their efforts to seek refunds. *See, e.g.* PX1 ¶¶8-11 [ER0896-97]; PX5 ¶¶8-12 [ER0978-80]; PX6 ¶¶7-9 [ER0989-90]. And Hardwire's argument that it should be allowed to continue its deception overseas so that duped foreign consumers might subsidize the restitution of domestic consumers belies its professed concern about international comity and ignores that the SAFE WEB Act allows the FTC to seek redress for foreign consumers. The district court properly determined that applying a preliminary injunction to Hardwire's foreign business is in the public interest, and the injunction is appropriately tailored to encompass all the conduct and all the remedies covered by the SAFE WEB Act.

CONCLUSION

The judgment of the district court should be affirmed.

Respectfully submitted,

ALDEN F. ABBOTT
General Counsel

JOEL MARCUS
Deputy General Counsel

October 22, 2018

/s/ Olga Vaytsman
OLGA VAYTSMAN
MICHELE ARINGTON
Attorneys

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Of Counsel:
SAMANTHA GORDON
MATTHEY H. WERNZ
Attorneys

FEDERAL TRADE COMMISSION
230 S. Dearborn Street, Suite 303
Chicago, IL 60604

STATEMENT OF RELATED CASES

Pursuant to Ninth Circuit Rule 28-2.6, I certify that there are no known related cases pending in this Court.

October 22, 2018

/s/ Olga Vaytsman

Olga Vaytsman
Attorney
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Form 8. Certificate of Compliance Pursuant to 9th Circuit Rules 28.1-1(f), 29-2(c)(2) and (3), 32-1, 32-2 or 32-4 for Case Number 18-56161

Note: This form must be signed by the attorney or unrepresented litigant *and attached to the end of the brief.*

I certify that (*check appropriate option*):

☐ This brief complies with the length limits permitted by Ninth Circuit Rule 28.1-1.
The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☒ This brief complies with the length limits permitted by Ninth Circuit Rule 32-1.
The brief is [9813] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☐ This brief complies with the length limits permitted by Ninth Circuit Rule 32-2(b).
The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable, and is filed by (1) ☐ separately represented parties; (2) ☐ a party or parties filing a single brief in response to multiple briefs; or (3) ☐ a party or parties filing a single brief in response to a longer joint brief filed under Rule 32-2(b). The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☐ This brief complies with the longer length limit authorized by court order dated [ ]
The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6). The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable.

☐ This brief is accompanied by a motion for leave to file a longer brief pursuant to Ninth Circuit Rule 32-2 (a) and is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32 (f), if applicable. The brief's type size and type face comply with Fed. R .App. P. 32(a)(5) and (6).

☐ This brief is accompanied by a motion for leave to file a longer brief pursuant to Ninth Circuit Rule 29-2 (c)(2) or (3) and is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

☐ This brief complies with the length limits set forth at Ninth Circuit Rule 32-4.
The brief is [ ] words or [ ] pages, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

Signature of Attorney or Unrepresented Litigant: s/ Olga Vaytsman

Date: Oct 22, 2018

("s/" plus typed name is acceptable for electronically-filed documents)

9th Circuit Case Number(s) 18-56161

NOTE: To secure your input, you should print the filled-in form to PDF (File > Print > *PDF Printer/Creator*).

****

CERTIFICATE OF SERVICE
When All Case Participants are Registered for the Appellate CM/ECF System

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on (date) Oct 22, 2018 .

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Signature (use "s/" format) s/ Olga Vaytsman

****

CERTIFICATE OF SERVICE
When Not All Case Participants are Registered for the Appellate CM/ECF System

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on (date) .

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within 3 calendar days to the following non-CM/ECF participants:

Signature (use "s/" format)