

No. 21-55099

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

JOHN MCCURLEY AND DAN DEFOREST,
INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY
SITUATED
Plaintiffs-Appellants,

v.

ROYAL SEAS CRUISES, INC.,
Defendants-Appellees.

On Appeal from the United States District Court
for the Southern District of California
No. 3:17-cv-00986-BAS-AGS
The Honorable Cynthia A. Bashant, District Court Judge

**BRIEF OF THE ELECTRONIC PRIVACY INFORMATION
CENTER AND THE NATIONAL CONSUMER LAW CENTER AS
AMICI CURIAE IN SUPPORT OF PLAINTIFFS-APPELLANTS
AND REVERSAL**

Alan Butler
Megan Iorio
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
iorio@epic.org

Attorneys for Amici Curiae

August 9, 2021

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *Amici Curiae* the Electronic Privacy Information Center and the National Consumer Law Center state that neither have parent corporations and that no publicly held corporation owns 10% or more of either of their stock.

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT.....	i
INTEREST OF THE <i>AMICI CURIAE</i>	1
SUMMARY OF ARGUMENT	4
ARGUMENT	7
I. SELLERS LIKE ROYAL SEAS CRUISES OUGHT TO KNOW THAT THERE IS A SIGNIFICANT RISK THAT THE CONSENT That LEAD GENERATORS OBTAIN IS NOT TCPA-COMPLIANT.....	7
A. Sellers use webs of contractors and sub-contractors to insulate themselves from liability for illegal robocalls made on their behalf.	9
B. Lead generation produces millions of illegal robocalls in recent years	14
C. Lead generators’ data collection practices are deceptive and do not reflect consent to be called by upstream telemarketers.....	17
D. Lead generator data is not only deceptively obtained but may also be riddled with errors and false data due to a lack of validation	28
II. A SELLER IS VICARIOUSLY LIABLE FOR ILLEGAL CALLS MADE BY CONTRACTORS HIRED TO ROBOCALL ON THEIR BEHALF WHEN THE SELLER DOES NOT EFFECTIVELY OVERSEE TCPA COMPLIANCE	32
A. The TCPA protects important consumer privacy rights by requiring companies to obtain consent prior to robocalling.....	33

B. Sellers cannot avoid TCPA liability by outsourcing compliance to third parties35

CONCLUSION.....38

CERTIFICATE OF COMPLIANCE.....39

CERTIFICATE OF SERVICE40

TABLE OF AUTHORITIES

Cases

<i>Barrera v. Guaranteed Rate, Inc.</i> , No. 17-cv-5668, 2017 WL 4837597 (N.D. Ill. Oct. 23, 2017).....	21
<i>Bell v. Royal Seas Cruises, Inc.</i> , No. 19-cv-60752, 2020 WL 5639947 (S.D. Fla. Sept. 21, 2020)	17
<i>Berman v. Freedom Fin. Network, LLC</i> , 400 F. Supp. 3d. 964 (N.D. Cal. 2019)	14, 17, 19
<i>Braver v. NorthStar Alarm Servs., LLC</i> , No. 17-cv-0383, 2019 WL 3208651 (W.D. Okla. July 16, 2019).....	15
<i>Cellco P’ship v. Plaza Resorts Inc.</i> , No. 12-cv-81238, 2013 WL 5436553 (S.D. Fla. Sept. 27, 2013)	14, 17
<i>Clough v. Revenue Frontier, LLC</i> , No. 17-cv-411, 2019 WL 2527300 (D.N.H. June 19, 2019)	13
<i>Cunningham v. Rapid Response Monitoring Servs., Inc.</i> , 251 F. Supp. 3d 1187 (M.D. Tenn. 2017)	24
<i>Desai v. ADT Security Sys. Inc.</i> , 78 F. Supp. 3d 896 (N.D. Ill. 2015)	13, 14, 20
<i>Evans v. Nat’l Auto Div., LLC</i> , No. 15-cv-8714, 2016 WL 4770033 (D.N.J. Sept. 13, 2016).....	19
<i>Heaton v. Motor Vehicle Assurance</i> , No. 17-cv-40169, 2018 WL 4696751 (D. Mass. Sept. 28, 2018)	19, 24
<i>Katz v. Liberty Power Corp., LLC</i> , No. 18-cv-10506, 2019 WL 4645524 (D. Mass. Sept. 24, 2019)	25
<i>Kristensen v. Credit Payment Servs.</i> , 879 F.3d 1010 (9th Cir. 2018).....	15, 17
<i>Kristensen v. Credit Payment Servs.</i> , No. 12-cv-00528, 2015 WL 4477425 (D. Nev. July 20, 2015), <i>aff’d</i> <i>on other grounds</i> , 879 F.3d 1010 (9th Cir. 2018)	13
<i>Pascal v. Agentra, LLC</i> , No. 19-cv-02418, 2019 WL 5212961 (N.D. Cal. Oct. 16, 2019)	17

<i>Pierucci v. Homes.com, Inc.</i> , No. 20-cv-455, 2020 WL 7647636 (E.D. Va. Dec. 23, 2020).....	23
<i>Rogers v. Interstate Nat’l Dealer Servs. Inc.</i> , No. 20-cv-00554, 2020 WL 4582689 (N.D. Ohio Aug. 10, 2020).....	17
<i>Satterfield v. Simon & Schuster, Inc.</i> , 569 F.3d 946 (9th Cir. 2009).....	21
<i>Seri v. Crosscountry Mortg., Inc.</i> , No. 16-cv-01214, 2016 WL 5405257 (N.D. Ohio Sept. 28, 2016)....	24
<i>Shuckett v. DialAmerica Mktg., Inc.</i> , No. 17-cv-2073, 2019 WL 3429184 (S.D. Cal. July 30, 2019).....	24
<i>Toney v. Quality Res., Inc.</i> , 75 F. Supp. 3d 727 (N.D. Ill. 2014)	20
<i>Turner v. eFinancial, LLC</i> , No. 18-cv-00292, 2018 WL 11182739 (D. Colo. Sept. 27, 2018).....	19
<i>Williams v. Pillpack LLC</i> , No. 19-cv-5282, 2021 WL 535215 (W.D. Wash. Feb. 12, 2021).12, 13	
Statutes	
Communications Act of 1934, ch. 652, Tit. II, 48 Stat. 1070 (47 U.S.C. 201 et seq.):	
47 U.S.C. § 227(b)(3).....	34
47 U.S.C. § 227(b)(4).....	34
47 U.S.C. § 227(g).....	34
Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, 105 Stat. 2394:	
TCPA §2, ¶¶1, 3.....	34
Other Authorities	
Campaign Monitor, <i>Email Marketing Terms: Double Opt-In</i> (2020)	31
Consumer Products USA, consumerproductsusa.com.....	22
Dep’t of Justice, <i>Telephone Robocall Abuse Criminal Enforcement and Deterrence Act: 2020 Report to Congress</i> (2020).....	16

Diabetes Health Info, diabeteshealth.info.....	21, 25
<i>FTC v. Career Educ. Corp.</i> , No. 19-cv-05739 (N.D. Ill. filed Aug. 27, 2019).....	16
<i>FTC v. Day Pacer LLC</i> , No. 19-cv-01984 (N.D. Ill. filed Mar. 22, 2019)	20
<i>FTC v. Expand, Inc.</i> , No. 16-cv-00714 (M.D. Fla. filed Apr. 28, 2016).....	27
<i>FTC v. Grand Bahama Cruise Line, LLC</i> , No. 20-cv-52 (M.D. Fla. filed Jan. 10, 2020).....	16, 17
<i>FTC v. Intermundo Media, LLC</i> , No. 14-cv-2529 (D. Colo. filed Sept. 12, 2014)	26
<i>FTC v. Ryan Golembiewski</i> , No.12-cv-00893 (S.D. Ohio filed Oct. 17, 2012)	27
FTC, <i>Big Print. Little Print. What’s the Deal?</i> (2000)	22
FTC, <i>Career Education Corporation Refunds</i> (June 2021).....	15
FTC, <i>Follow the Lead: An FTC Workshop on Lead Generation</i> (Oct. 2015).....	11, 12, 26, 31
FTC, <i>Staff Perspective: “Follow the Lead” Workshop</i> (Sep. 2016) ...	passim
Google, <i>reCAPTCHA Help</i> (2021)	30
H.R. Rep. No. 102-317 (1991)	34
Homes.com	23
IDology, <i>Enhanced Phone Number Verification</i> (2021).....	31
<i>In re Joint Petition Filed by Dish Network, LLC</i> , 28 F.C.C. Rcd. 6574 (2013)	35, 36, 37
Instant Play Giveaway Entry, instantpaygiveawayentry.com.....	21
Lending Tree, <i>Partner Listing</i> (2021)	23
Lesley Fair, FTC, <i>Full Disclosure</i> (Sept. 23, 2014).....	22
Mortgage Rsch. Ctr., <i>Our Home Services Partners</i> (2021).....	23
Mortgage Rsch. Ctr., <i>Our Network Members</i> (2021)	23

Randall-Reilly, randallreilly.com	25
Retail Product Zone, retailproductzone.com	22
S. Rep. No. 102-177 (1991)	33
Thor Olavsdud, <i>How Businesses Can Get Consumers to Share Their Data</i> , CIO (Jul. 20, 2012).....	29
<i>United States v. GoLoansOnline.com</i> , No. 14-cv-1262 (S.D. Tex. filed May 7, 2014).....	27
<i>United States v. KFJ Marketing, LLC</i> , No. 16-cv-1643 (C.D. Cal. filed Mar. 10, 2016).....	15
We Have Auto Loans, wehaveautoloans.com	24

INTEREST OF THE *AMICI CURIAE*¹

The Electronic Privacy Information Center (“EPIC”) is a public interest research center in Washington, D.C., that focuses public attention on emerging privacy and civil liberties issues in the information age. EPIC routinely participates as *amicus curiae* in cases concerning the Telephone Consumer Protection Act. *See* Br. for NCLC & EPIC as *Amici Curiae* Supporting Appellant, *Lindenbaum v. Realgy, LLC*, No. 20-4252 (6th Cir. filed Feb. 1, 2021); Br. for EPIC et al. as *Amici Curiae* Supporting Respondent, *Facebook, Inc., v. Duguid*, 141 S. Ct. 1163 (2020) (No. 19-511); Br. for EPIC et al. as *Amici Curiae* Supporting Petitioner, *Barr v. Am. Ass’n of Political Consultants, Inc.*, 140 S. Ct. 2335 (2020) (No. 19-631); Br. for EPIC as *Amicus Curiae* Supporting Respondent, *PDR Network v. Carlton & Harris Chiropractic*, 139 S. Ct. 2051 (2019) (No. 17-1705); Br. for EPIC &

¹ The parties consent to the filing of this *amicus curiae* brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party. EPIC clerks Alexa Daugherty, Soojin Jeong, and Nicole Mo contributed to this brief.

NCLC as *Amici Curiae* Supporting Appellant, *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458 (7th Cir. 2020) (No. 19-1738); Br. for EPIC as *Amicus Curiae* Supporting Appellee, *Gallion v. United States*, 772 Fed. App'x. 604 (9th Cir. 2019) (No. 18-55667); Br. for EPIC et al. as *Amici Curiae* in Support of Respondents, *ACA Int'l v. FCC*, 885 F.3d 687 (D.C. Cir. 2018) (No. 15-1221).

The National Consumer Law Center (“NCLC”) is a national research and advocacy organization focusing on justice in consumer transactions, especially for low-income and elderly consumers. Attorneys for NCLC have advocated extensively on behalf of consumers to protect their interests related to robocalls before the United States Congress, the Federal Communications Commission (FCC), and the federal courts. These activities have included testifying in numerous hearings before various Congressional committees regarding how to control invasive and persistent robocalls, many filings and appearances before the FCC urging strong interpretations of the Telephone Consumer Protection Act (“TCPA”), and the filing of amicus briefs before the federal courts of appeals representing the interests of consumers regarding the TCPA. NCLC also publishes and regularly

updates a comprehensive analysis on the laws governing robocalls in National Consumer Law Center, *Federal Deception Law*, Chapter 6 (3d ed. 2017), updated at www.nclc.org/library.

SUMMARY OF ARGUMENT

Royal Seas Cruises wants all of the advantages of robocalling people with none of the responsibilities. The Telephone Consumer Protection Act (“TCPA”) was meant to put a stop to this behavior. The TCPA requires companies that wish to robocall people to obtain prior express written consent. But Royal Seas Cruises did not obtain the required consent. Instead, it contracted with Prospects DM, which contracted with several other companies, to generate new customer contacts—called “leads”—and obtain their consent to receive robocalls.

However, no one in the supply chain obtained consent from the plaintiffs. This should not have been a surprise to Royal Seas Cruises—this kind of behavior is rampant in the lead generation industry and is a known risk when obtaining leads online. Royal Seas Cruises should not be able to escape liability for the illegal robocalls because of a boilerplate contract provision and willful blindness to its supply chain of marketing leads.

Contact data from lead generators has been used to make millions of illegal robocalls in recent years. The FTC has been investigating the industry for several years and has filed lawsuits against

paradigmatically unscrupulous lead generators. Lead generators often use deceptive or misleading premises to lure in leads—like free giveaways or help selecting a complicated product (e.g. insurance). The contact information these lead generators collect is also inherently unreliable because anyone—even a bot—can submit information in a web form. Lead generators, like the ones at the center of this case, often do little (if anything) to verify the information they collect is accurate. Sellers attempt to shield themselves from the underworld of lead generation by hiring long chains of contractors and failing to investigate their lead supply chains.

But sellers should not be given a free pass when their contractors break the law. Any interpretation of vicarious liability under the TCPA must be consistent with the law’s goal: to protect consumer privacy. The TCPA accomplishes this goal by requiring companies to obtain consent before they robocall. But enforcement is essential to TCPA compliance. Companies only comply with the TCPA because they face potential legal action from consumers, state attorneys general, and the FCC, all of which carry hefty penalties.

If sellers who contract with third party telemarketers to robocall leads on their behalf can insulate themselves from liability with a simple contract provision and ignorance of their specific lead supply chain, it will turn into a recipe for evading the TCPA—and other sellers will likely follow. Sellers will continue to employ unscrupulous telemarketers because their incentive *not* to do so—the risk of TCPA enforcement—will no longer exist. And unscrupulous telemarketers will simply locate themselves overseas, as many already do, where they cannot be hauled into U.S. courts to face enforcement. The result will be to dramatically weaken TCPA enforcement, denying consumers any remedy for their privacy injuries, and leaving consumers unprotected from future harms.

This is precisely why the FCC has said that sellers are in the best position to ensure that leads are collected in a TCPA-compliant manner. Sellers must be incentivized to know their supply chain and to make careful decisions about who to employ to ensure TCPA compliance. Sellers' decisions will have a greater impact on consumer privacy than whack-a-mole litigation against unscrupulous lead generators who will continue to enter the market as long as there is a demand for their

services. This Court should not allow Royal Seas Cruises to use a contract clause to insulate itself from liability for the illegal and intrusive telemarketing conducted on its behalf.

ARGUMENT

I. SELLERS LIKE ROYAL SEAS CRUISES OUGHT TO KNOW THAT THERE IS A SIGNIFICANT RISK THAT THE CONSENT THAT LEAD GENERATORS OBTAIN IS NOT TCPA-COMPLIANT.

Lead generation is the process by which companies acquire new customer contact information. Telemarketers have long relied on lead generation to find new customers. But today, lead generation is a heavily data-driven industry that involves various actors that collect, aggregate, enrich, and package leads for sale. Sellers that rely on telemarketing employ contractors to make the calls, who themselves employ additional contractors to aggregate leads for them, and on and on, down to the last sub-contractor who actually collects the lead.

At some point in this process, someone must also collect express written consent from the leads before robocalling them. But, as a slew of recent cases show, the TCPA's consent requirement often gets lost in the mix. Poor or nonexistent compliance mechanisms have led to millions of illegal robocalls over the last few years. Sellers attempt to

insulate themselves from liability by remaining ignorant of their specific supply chains—and thus fail to supervise TCPA compliance.

Failure to supervise the compliance of contractors has allowed companies with deceptive and unreliable consent acquisition methods to proliferate throughout the market. Web publishers in the lead generation space routinely use deceptive or misleading methods to trick consumers into providing their contact information and to be robo-called by hundreds or even thousands of unrelated companies. These web publishers also often do not do enough to validate that the consent they received is real and not the result of someone—or something, like a bot—submitting false information. The TCPA requires them to do more—but sellers are not requiring it, because they believe they are shielded from liability.

Sellers that contract with third parties to robo-call leads on their behalf must be aware of the vast level of fraud and deception that pervades the lead generation industry. The FTC has been investigating the industry for years. The FTC held a consumer protection workshop on online lead generation in October 2015 and issued a staff paper on lead generation in September 2016. Information on unscrupulous

practices was readily available when Royal Seas Cruises had the plaintiffs in this case robocalled with leads from unscrupulous web publishers.

Sellers know, or ought to know, that lead generators cannot be trusted to obtain consent in compliance with the TCPA without supervision. Sellers cannot use ignorance of their specific supply chains to claim ignorance of well-known industry practices. This Court should not allow Royal Seas Cruises to use boilerplate contract clauses to shield itself from liability for the tens of thousands of illegal robocalls it caused to be made on its behalf.

A. Sellers use webs of contractors and sub-contractors to insulate themselves from liability for illegal robocalls made on their behalf.

The lead generation industry collects, sells, aggregates, and resells consumer information for profit. The web of companies involved in supplying a seller with leads is generally long and convoluted. Sellers purposefully shield themselves from knowledge of their own supply chain and seek to insulate themselves from liability with boilerplate contract clauses that purport to make TCPA compliance someone else's problem. But sellers like Royal Seas Cruises who have used

telemarketing for decades understand that the telemarketing companies they employ use networks of sub-contractors to supply them with leads, and that many of these sub-contractors are untrustworthy. Sellers cannot use ignorance of the specifics of their supply chain to escape liability when they purposefully engage with an industry that is notoriously fraudulent and deceptive.

Telemarketing lead generation generally starts at a web form owned by a web publisher. FTC, *Staff Perspective: “Follow the Lead” Workshop 2* (Sep. 2016) [FTC September 2016 Staff Perspective].² Potential customers (“leads”) land on websites with forms that incentivize them to fill out information about themselves to register for a sweepstakes or learn more about a service they are seeking. *Id.* The web form may simply request an individual’s name and contact information or may request extensive personal information, such as a Social Security number and birth date. *Id.*

² Available at https://www.ftc.gov/system/files/documents/reports/staff-perspective-follow-lead/staff_perspective_follow_the_lead_workshop.pdf.

Next in the lead generation pipeline is the lead aggregator, a company that aggregates leads from a large network of websites and then sells the information to merchants or other aggregators. FTC September 2016 Staff Perspective at 3. An individual's information is rarely sold or rented once, but rather circulated multiple times to various requesting entities—adding layers of opacity to the lead generation transaction process. *Id.* at 5; *See also* FTC, *Follow the Lead: An FTC Workshop on Lead Generation* 76 (Oct. 2015) [FTC October 2015 Workshop].³ Unless aggregators are also web publishers, their presence is rarely consumer-facing, making these companies largely invisible and unknown to consumers.

Telemarketers obtain leads from aggregators and then call the leads to promote a given product or service before passing the lead on to a seller. FTC October 2015 Workshop at 20. At the top of the chain are the sellers, who contract with telemarketers to call leads on their behalf. Sellers sometimes include provisions in their contracts requiring

³ *Available at* <https://www.ftc.gov/system/files/documents/videos/follow-lead-ftc-workshop-lead-generation-part-1/lgw-transcript-pt1.pdf>.

the telemarketer to comply with the TCPA but fail to supervise compliance even when the contract specifically allows for such supervision—such as in the present case.

The number of companies and websites involved in generating leads for a single seller’s campaign can be massive and often increases exponentially as one moves down the chain. *See* FTC October 2015 Workshop at 25–26 (describing how one seller can receive contacts from “hundreds, thousands, or millions of websites” because of the “one-to-many” relationship of aggregators to web publishers and how that adds to the “risk” of using lead generators). The lead generation ecosystem in *Williams v. Pillpack LLC*, No. 19-cv-5282, 2021 WL 535215 (W.D. Wash. Feb. 12, 2021)—which also involved the telemarketer in this case, Prospects DM—is an illustrative example. First, Pillpack, a full-service pharmacy and the seller in this story, hired an independent contractor, Performance Media Services, to generate leads. *Id.* at *1. Performance Media then engaged Prospects DM to place calls and transfer them to Pillpack’s call center. *Id.* To make these calls, Prospects DM bought contact information from three lead aggregation companies—Little Brook Media, Sharecare Inc, and Yodel Technologies

LLC—that collectively operated dozens of websites to collect consumer information. *Id.* Yodel also obtained contact information from a fourth lead aggregator, Fluent Inc. *Id.*

This process of contracting and subcontracting out lead generation to a large network of call centers, lead aggregators and web publishers is common. *See, e.g., Clough v. Revenue Frontier, LLC*, No. 17-cv-411, 2019 WL 2527300, at *1 (D.N.H. June 19, 2019) (noting that a text message promoting tax relief services involved five layers of call centers and lead generators, including an “affiliate network” of generators and publishers that collected consumer information); *Kristensen v. Credit Payment Servs.*, No. 12-cv-00528, 2015 WL 4477425, at *1 (D. Nev. July 20, 2015) (describing a lead generator contracting with a sub-generator who worked with “thousands of small companies” to generate and order leads for a payday loan company), *aff’d on other grounds*, 879 F.3d 1010 (9th Cir. 2018); *Desai v. ADT Security Sys. Inc.*, 78 F. Supp. 3d 896, 899–901 (N.D. Ill. 2015) (describing a web publisher, 2freenights.com, that directly obtained leads from its websites and also purchased leads from 20-30 additional unidentified lead generation websites, then sold the leads to Europe Media International, which then sold the leads to

Paramount Media Group, which was one of five to ten companies that sold leads to the marketing company, the Elephant Group, for ADT's marketing campaign).

B. Lead generation produces millions of illegal robocalls in recent years.

Purchased leads have been at the center of cases involving thousands and even millions of illegal robocalls. The FTC has taken action against sellers and lead generators in an effort to reign in the industry's deceptive practices. Untrustworthy lead generators are especially common in certain industries and have fueled expansive illegal robocall campaigns.

In recent years, lawsuits involving lead generators have exposed tens of thousands and even millions of illegal robocalls. *See Celco P'ship v. Plaza Resorts Inc.*, No. 12-cv-81238, 2013 WL 5436553, at *2 (S.D. Fla. Sept. 27, 2013) (finding 5,785,245 robocalls promoting seller's travel services); *Desai*, 78 F. Supp. at 901 (finding nearly 3.8 million illegal robocalls made on behalf of ADP); *Berman v. Freedom Fin. Network, LLC*, 400 F. Supp. 3d. 964, 977 (N.D. Cal. 2019) (finding "millions" of robocalls made promoting debt-relief services of a single seller, including 989,295 robocalls to the 149,838 putative class

members); *Braver v. NorthStar Alarm Servs., LLC*, No. 17-cv-0383, 2019 WL 3208651, at *4 (W.D. Okla. July 16, 2019) (concerning 252,765 illegal robocalls); *Kristensen v. Credit Payment Servs.*, 879 F.3d 1010 (9th Cir. 2018) (concerning unlawful automated texts sent to almost 100,000 people).

The FTC has brought enforcement actions against sellers for using deceptive lead generation to make illegal robocalls. In 2016, the FTC brought an action in federal court against lead generator companies who had placed more than 1.3 million illegal robocalls on behalf of solar panel installation companies. Compl. at 6, *United States v. KFJ Marketing, LLC*, No. 16-cv-1643 (C.D. Cal. Mar. 10, 2016). The agency has recently settled and paid out nearly \$30 million to more than 8,000 people who had been subject to Career Education Corporation and other secondary education companies' deceptive lead generation practices. FTC, *Career Education Corporation Refunds* (June 2021);⁴ see *FTC v.*

⁴ <https://www.ftc.gov/enforcement/cases-proceedings/refunds/career-education-corporation-refunds>.

Career Educ. Corp., No. 19-cv-05739 (N.D. Ill. filed Aug. 27, 2019).⁵ The FTC has also filed suit against Grand Bahama Cruise Line and others for making millions of illegal robocalls using purchased leads. *FTC v. Grand Bahama Cruise Line, LLC*, No. 20-cv-52 (M.D. Fla. filed Jan. 10, 2020).⁶ The FTC's recent enforcement actions are part of a joint federal, state, and local effort called Operation Call It Quits, which demonstrates the scale at which lead generators perpetuate and exacerbate the robocalling problem and the known risk of employing lead generators to obtain TCPA consent. Dep't of Justice, *Telephone Robocall Abuse Criminal Enforcement and Deterrence Act: 2020 Report to Congress*, at 6–7 (2020).⁷

While lead generation is a popular marketing strategy across industries, a few sectors are heavily represented in TCPA case law involving lead generators. Both health and automotive insurance

5

https://www.ftc.gov/system/files/documents/cases/career_education_corporation_complaint_8-27-19.pdf.

⁶ www.ftc.gov/enforcement/cases-proceedings/162-3005/grand-bahama-cruise-line-llc.

⁷ <https://www.justice.gov/opa/press-release/file/1331576/download>.

companies are common parties in robocall litigation. *See, e.g., Pascal v. Agentra, LLC*, No. 19-cv-02418, 2019 WL 5212961 (N.D. Cal. Oct. 16, 2019) (health insurance); *Rogers v. Interstate Nat'l Dealer Servs. Inc.*, No. 20-cv-00554, 2020 WL 4582689 (N.D. Ohio Aug. 10, 2020) (automotive protection plans). Loan agencies and debt relief providers also regularly use illegal lead generation practices. *See, e.g., Kristensen*, 879 F.3d 1010 (loan agency); *Berman*, 400 F. Supp. 3d. 964 (debt relief). The travel industry, especially cruise lines, are another sector disproportionately represented in TCPA robocall litigation. *See, e.g., Plaza Resorts*, No. 12-cv-81238, 2013 WL 5436553 (resort and cruise companies); *Bell v. Royal Seas Cruises, Inc.*, No. 19-cv-60752, 2020 WL 5639947 (S.D. Fla. Sept. 21, 2020) (cruise company); *FTC v. Grand Bahama Cruise Line, LLC*, No. 20-cv-52 (M.D. Fla. filed Jan. 10, 2020) (cruise companies).

C. Lead generators' data collection practices are deceptive and do not reflect consent to be called by upstream telemarketers.

It is not surprising that use of lead generator call lists has led to millions of illegal robocalls because the underlying data collection practices of these companies are deceptive and untrustworthy. Lead

generating websites are often designed to trick visitors into providing their contact information based on false promises and elusive monetary rewards. And even when lead generators expressly request contact information for product marketing purposes, they frequently send that information along to companies that offer entirely unrelated products or services. These bait-and-switch tactics are inherently deceptive, and sellers should not be allowed to treat the records they generate as reliable indications of express consent to be called. Royal Seas Cruises should have been aware of the risks involved in using online generated leads and should have investigated its supply chain to ensure that the websites used to generate its leads were not inherently misleading—and thus untrustworthy.

Lead generator websites use a variety of tactics to lure people in. Some web publishers offer rewards or free products that ultimately prove elusive. For instance, one website, rewardzoneusa.com, offers \$100 gift cards in exchange for responses to a lengthy consumption survey, and then forces people to provide their phone number to claim the gift card—along with consent to be robocalled from various companies offering job search, debt, medical, college, and insurance

help, along with various other services. *See Berman*, 400 F. Supp. at 984 (finding a triable issue whether rewardzoneusa.com and another website offering free products, signup.electronics-sweepstakes.com, mislead visitors into signing up for robocalls). Many others purportedly offer easy comparisons for complex purchases, such as insurance or loans, but then turn around and sell peoples' data to a slew of unrelated companies that then robocall them endlessly. *See, e.g., Turner v. eFinancial, LLC*, No. 18-cv-00292, 2018 WL 11182739, at *3 (D. Colo. Sept. 27, 2018) (involving insurancequotes.com, which advertises insurance rate quotes, but sold leads to companies that provide other services, such as solar panels, as well as generic marketing firms); *Heaton v. Motor Vehicle Assurance*, No. 17-cv-40169, 2018 WL 4696751 (D. Mass. Sept. 28, 2018) (involving wehaveautoloans.com, whose leads are sold to "1800CARSHOW, Detroit Trading, DriveTime, Sunrise Media Partners and other third parties"); *Evans v. Nat'l Auto Div., LLC*, No. 15-cv-8714, 2016 WL 4770033, at *1 (D.N.J. Sept. 13, 2016) (leads from directautowarranty.co sold to "up to 5 partners from our network" without further explication of those "partners").

Lead generators also frequently collect and sell information based on pretexts that have little or no connection to the products companies eventually market to individuals. *See* Compl. for Civil Penalties, Permanent Inj., and Other Relief at 14, *FTC v. Day Pacer LLC*, No. 19-cv-01984 (N.D. Ill. filed Mar. 22, 2019) (alleging that defendant lead generation company called an individual to provide information on higher education though the individual had submitted a web form to receive information on insurance benefits);⁸ *see also* FTC September 2015 Staff Perspective at 4 (“in some past instances aggregators have sold [leads] to clients who offered consumers alternative products they did not apply for.”). For example, web forms related to children’s slippers have resulted in individuals’ contact information being sold to advertisers for pharmaceutical products. *Toney v. Quality Res., Inc.*, 75 F. Supp. 3d 727, 731–32 (N.D. Ill. 2014). Web forms for travel have led to phone calls from home security system marketers. *See Desai*, 78 F. Supp. 3d at 901. And sites advertising free ringtones have led to

8

https://www.ftc.gov/system/files/documents/cases/edutrek_complaint.pdf

robocalls from publishing houses promoting major book releases.

Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 949 (9th Cir. 2009).

Many lead generating web publishers also target vulnerable groups, such as senior citizens, people with chronic medical conditions, or people living paycheck to paycheck. One of the websites at the center of this case is a prime example: diabeteshealth.info. The site appeals to individuals looking to reduce the costs of their diabetes supplies—and then sells their contact information to various companies marketing goods that have nothing to do with diabetes supplies.

Lead generators design their sites in ways that deceptively obfuscate the mandatory TCPA disclosures and opt-in processes. The opt-in language is often presented in tiny, light-colored print; the list of companies that the website sells leads to can be hidden away on a separate page and be hundreds or thousands of companies long; and the list of companies is presented in impenetrable blocks of text or small print. *See, e.g., Barrera v. Guaranteed Rate, Inc.*, No. 17-cv-5668, 2017 WL 4837597, at *1 (N.D. Ill. Oct. 23, 2017) (disclosures and use of tiny font made it unlikely plaintiff knew what he was consenting to); *See also* Instant Play Giveaway Entry (listing opt-in information on some

survey questions and at the end of the survey in light-grey font with a link to the companies it sells leads to);⁹ Consumer Products USA (listing Marketing Partners in a hyperlink at the end of a survey, but not in the Privacy Policy or Terms & Conditions);¹⁰ Retail Product Zone (hyperlinking thousands of marketing partners in an opt-in form).¹¹

The Federal Trade Commission has made clear in the marketing context that the use of small fonts and other tactics to obscure the true cost of a product or nature of a transaction can be deceptive. *See* FTC, *Big Print. Little Print. What's the Deal?* (2000).¹² Specifically, the FTC has said that if “disclosure of information necessary to prevent an ad from being deceptive, the disclosure has to be clear and conspicuous.” Lesley Fair, FTC, *Full Disclosure* (Sept. 23, 2014).¹³ The intentional obfuscation of a TCPA opt-in on a lead generator intake form is

⁹ <http://instantplaygiveawayentry.com>.

¹⁰ <https://www.consumerproductsusa.com>.

¹¹ <http://retailproductzone.com>.

¹² <https://www.ftc.gov/system/files/documents/plain-language/bus44-big-print-little-print-whats-deal.pdf>.

¹³ <https://www.ftc.gov/news-events/blogs/business-blog/2014/09/full-disclosure>.

precisely the type of deceptive business practice that the FTC has called out for many years.

One particularly egregious example is Homes.com, which has opt-in language (all in small, light-grey font) stating that submitting is consent to be contacted “by participating members of the Mortgage Research Center, LLC network and providers of home-related services, even if I am on the Do Not Call List.” *See Pierucci v. Homes.com, Inc.*, No. 20-cv-455, 2020 WL 7647636, at *2 (E.D. Va. Dec. 23, 2020). The phrase “home-related services” is a hyperlink listing ten entities. Mortgage Rsch. Ctr., *Our Home Services Partners* (2021).¹⁴ The phrase “participating members” is a hyperlink to a list of 408 entities. Mortgage Rsch. Ctr., *Our Network Members* (2021).¹⁵ At the bottom of this page is yet another hyperlink to a list of the Lending Tree network, which can also receive leads from Homes.com. The Lending Tree list is 2493 entities long. Lending Tree, *Partner Listing* (2021).¹⁶

¹⁴ https://www.mortgageresearchcenter.org/home-services-partners/#skip_to_content.

¹⁵ https://www.mortgageresearchcenter.org/partners/#skip_to_content.

¹⁶ <https://www.lendingtree.com/legal/partner-list>.

Some web publishers also obfuscate who receives individuals' information. Publishers often have partial lists of affiliates on their websites or vaguely refer to "other[s]" who might receive an individual's data. *See e.g.*, We Have Auto Loans (informing consumers that their information will be shared with "other third parties");¹⁷ *Heaton*, No. 17-cv-40169, 2018 WL 4696751, at *2 (case against a company that used leads from wehaveautoloans.com).

The calls generated from a single contact form can be relentless and sometimes impossible to stop. One plaintiff complained of receiving 28 telemarketing calls regarding home security systems from one submitted form, some only a second or two apart. *Cunningham v. Rapid Response Monitoring Servs., Inc.*, 251 F. Supp. 3d 1187, 1191 (M.D. Tenn. 2017); *see also Seri v. Crosscountry Mortg., Inc.*, No. 16-cv-01214, 2016 WL 5405257, *1 (N.D. Ohio Sept. 28, 2016) (plaintiff called at least 20 times); *Shuckett v. DialAmerica Mktg., Inc.*, No. 17-cv-2073, 2019 WL 3429184, at *1 (S.D. Cal. July 30, 2019) (plaintiff received around 40

¹⁷ <http://www.wehaveautoloans.com>.

pre-recorded telemarketing calls from Prospects DM, the telemarketer used in this case).

The number of potential calls is also not limited by the number of companies listed as “marketing partners” on these websites. Web publishers sell contact information to many different marketing companies and other lead aggregators, and those lists are ultimately used to fuel robocall campaigns on behalf of many more companies. *See* FTC September 2016 Staff Perspective at 3 (“Once an aggregator has processed a batch of leads . . . it may sell that batch to yet another aggregator.”); *see also* Diabetes Health Info (listing several companies with “marketing” in their name and a known lead aggregator, Liberty Power);¹⁸ *Katz v. Liberty Power Corp., LLC*, No. 18-cv-10506, 2019 WL 4645524 (D. Mass. Sept. 24, 2019) (TCPA suit against Liberty Power); Randall-Reilly (2021) (a marketing company listed as a “marketing partner” on several of the websites described in this brief, such as instantplaygiveawayentry.com and rewardzoneusa.com).¹⁹

¹⁸ <https://diabeteshealth.info>.

¹⁹ <https://www.randallreilly.com>.

The FTC held a workshop on lead generators in October 2015, before Royal Seas Cruises caused the named plaintiffs to be robocalled. At the outset, the FTC noted the role of lead generators in many fraud cases, particularly in debt relief scams, prepaid card scams, and sweepstakes fraud. FTC October 2015 Workshop at 8. One speaker whose company tracks marketing practices described how market pressures lead to aggressive (and misleading) practices in lead generation. *Id.* at 55–65. Other consumer protection advocates stressed the problem with “initial deceptions” used to lure in leads. *Id.* at 76–77.

The next year, the FTC issued a staff paper summarizing the main points of the workshop and summarized some of the deceptive and otherwise problematic marketing practices of lead generators. FTC September 2016 Staff Perspective at 6. The staff paper cited several enforcement actions taken against deceptive lead generators and the sellers that use them—all of which were filed before Royal Seas Cruises initiated its robocall campaign. *Id.*; see, e.g., *FTC v. Intermundo Media, LLC*, No. 14-cv-2529 (D. Colo. filed Sept. 12, 2014) (describing lead

generator that ran deceptive ads for “free” mortgage refinancing);²⁰ *United States v. GoLoansOnline.com*, No. 14-cv-1262 (S.D. Tex. filed May 7, 2014) (describing lead generator that used deceptive loan rates to lure in leads);²¹ *FTC v. Expand, Inc.*, No. 16-cv-00714 (M.D. Fla. filed Apr. 28, 2016) (concerning a lead generator advertising jobs that instead used leads to sell educational programs);²² *FTC v. Ryan Golembiewski*, No. 12-cv-00893 (S.D. Ohio filed Oct. 17, 2012) (describing a lead generator that deceptively claimed it could quickly reduce or eliminate consumer debts).²³ The agency warned that “companies who choose to ignore warning signs and look the other way may be at risk of violating the law themselves.” FTC September 2016 Staff Perspective at 7. Even if Royal Seas Cruises did not know that the specific websites collecting its leads advertised unrelated services or

²⁰ Available at <https://www.ftc.gov/enforcement/cases-proceedings/122-3225/intermundo-media-llc-delta-prime-refinance>.

²¹ Available at <https://www.ftc.gov/enforcement/cases-proceedings/122-3228/goloansonlinecom-inc>.

²² Available at <https://www.ftc.gov/enforcement/cases-proceedings/152-3124/expand-inc-gigats>.

²³ Available at <https://www.ftc.gov/enforcement/cases-proceedings/112-3079/golembiewski-ryan-united-debt-associates-llc-et-al>.

were otherwise untrustworthy, the company should have known that contracting for leads held a real risk that companies such as these would generate their leads.

Lead generation websites may be adept at collecting large volumes of data from unsuspecting internet users, but their deceptive business practices fundamentally undermine the reliability of the “consent” data that they obtain. Sellers and telemarketers should not be allowed to rely on consent representations made by these lead generators, especially when they do not take the basic technological steps necessary to verify the numbers and validate consent.

D. Lead generator data is not only deceptively obtained but may also be riddled with errors and false data due to a lack of validation.

There are simple steps that can be taken to verify and validate contact information given by a user online. But lead generators generally do not take these steps, and their failure to do so makes their representations about prior express consent inherently unreliable.

There is no guarantee that information submitted in a form is genuine—and there are many reasons to believe that the information is false or manufactured.

People are generally protective of their phone numbers and may provide a fake phone number when asked for their contact information—and that fake phone number may be someone else’s actual phone number. A PricewaterhouseCoopers study found that less than 18% of survey respondents were highly willing to share their cell phone number with a company—significantly less than the portion of people who were willing to share other personal information, such as their name, household income, birth date, or even their email address. Thor Olavsd, *How Businesses Can Get Consumers to Share Their Data*, CIO (Jul. 20, 2012).²⁴

People who do not trust a website may enter a fake phone number to see what happens when they submit the form—for example, if a website hawking insurance says that it will show the person quotes only if they enter their phone number. People are also likely to prefer to be contacted by email, and so may provide a real email address and a fake phone number if both forms of contact are requested.

²⁴ <https://www.cio.com/article/2393923/how-businesses-can-get-consumers-to-share-their-data.html>.

Another source of fake or manufactured leads are spam bots. Bots are computer programs that traverse websites and, in some cases, fill out and submit online forms. One indication that a spam bot submitted a set of form responses is that many entries have the same IP address—which blocks of the data set at issue in this case appear to have. *See* Appellant’s Br. at 19 n. 16.

There are many ways to minimize form spam. One of the most popular methods for blocking bot form submissions is a CAPTCHA, which is a piece of code embedded in a form that can tell the difference between a bot and a human by presenting a challenge that is designed to be easy for a human to solve but hard for a robot to solve. *See, e.g.,* Google, *reCAPTCHA Help* (2021).²⁵ Forms that do not have CAPTCHAs or other code-based bot barriers are more likely to receive spam leads. Yet, many lead generating websites—including diabeteshealth.info, one of the websites at the center of this case—do not have CAPTCHAs.

Lead generators can also filter out false or manufactured leads during or after collection by validating the submitted information. Tools

²⁵ <https://support.google.com/recaptcha>.

are available to validate that the name provided in an online form matches the provided phone number, along with other information, such as location. See, e.g., IDology, *Enhanced Phone Number Verification* (2021);²⁶ see also FTC October 2015 Workshop at 20–21, 32–33, 37, 66–68 (discussing the need for lead verification). The fact that so many of the leads provided to Prospects DM had unmatching contact names and phone numbers indicates that no one in the lead generation pipeline validated the data. Appellant’s Br. at 59.

Finally, lead generators can also verify lead data by simply contacting the lead via email or a non-robocall prior to robocalling them. Confirmed opt-in procedures (also called double opt-in) are routinely used for email list sign ups from online contact forms, even though there is no legal requirement to obtain prior express written consent to send a person a marketing email. Campaign Monitor, *Email Marketing Terms: Double Opt-In* (2020).²⁷

²⁶ <https://www.idology.com/identity-verification/enhanced-phone-verification/>.

²⁷ <https://www.campaignmonitor.com/resources/glossary/double-opt-in/>.

Lead generator practices create significant risks of obtaining false or inaccurate data. Given these risks, it is not reasonable to assume that lead generators' representations of having obtained prior express written consent are correct. Sellers like Royal Seas Cruises that do nothing to confirm and verify opt-ins are just as responsible as anyone else in the supply chain for the illegality of a call made using those leads.

II. A SELLER IS VICARIOUSLY LIABLE FOR ILLEGAL CALLS MADE BY CONTRACTORS HIRED TO ROBOCALL ON THEIR BEHALF WHEN THE SELLER DOES NOT EFFECTIVELY OVERSEE TCPA COMPLIANCE.

The lower court's failure to find vicarious liability for Royal Seas Cruises under any of Appellant's theories encourages behavior that contradicts the TCPA's statutory purposes and undermines TCPA compliance. Specifically, the lower court's decision encourages sellers to know as little as possible about their contractors' activities and to take a hands-off approach to TCPA compliance. This practically ensures that unscrupulous telemarketers and lead generators—particularly ones that cannot be hauled into a U.S. court—will predominate the lead generation industry, undermining the TCPA's important consumer protections.

This is the exact opposite of how the FCC has interpreted vicarious liability under the TCPA. The FCC has said that sellers can be held vicariously liable for their telemarketers' violations of the TCPA. The FCC recognized that sellers must be incentivized to know their supply chains and ensure that their contractors are complying with the TCPA. If Royal Seas Cruises, which explicitly contracted for robocalls to be made on its behalf but did practically nothing to ensure compliance, cannot be held vicariously liable, then vicarious liability for sellers will be drastically weakened. This Court should follow the FCC's analysis and hold that Royal Seas Cruises is vicariously liable under Appellant's proffered theories.

A. The TCPA protects important consumer privacy rights by requiring companies to obtain consent prior to robocalling.

Congress passed the TCPA to respond to the "national outcry" over unsolicited phone calls bombarding consumers' phone lines. S. Rep. No. 102-177, at 19 (1991). Congress found that prerecorded voice machines were allowing telemarketers to make calls without incurring "the normal cost of human intervention." H.R. Rep. No. 102-317, at 6

(1991). These “cost-effective” telemarketing tools incentivized high volume calling. TCPA §2, ¶¶1, 3.

Enter the TCPA and its prior express written consent requirement. The requirement that companies obtain prior express written consent before robocalling was meant to ensure that people are in control of who robocalls them and not the other way around. H.R. Rep. No. 102-317, at 6. The consent requirement also counteracts the telemarketer’s natural incentive to call as many individuals as possible. But the only reason companies comply with the TCPA is because Congress imposed hefty penalties for noncompliance and provided for several potential avenues for enforcement. See 47 U.S.C. § 227(b)(3) (providing for a private right of action to seek damages of \$500 per violation); 47 U.S.C. § 227(g) (empowering states attorneys general to bring TCPA actions for damages and injunctive relief); 47 U.S.C. § 227(b)(4) (authorizing the FCC to enforce the TCPA against violators). Without the threat of liability—without the threat of effective enforcement—companies have no incentive to comply and every incentive to call whatever telephone numbers they can get their hands on.

B. Sellers cannot avoid TCPA liability by outsourcing compliance to third parties.

When a seller employs a third-party telemarketer to robocall leads and fails to take concrete steps to ensure that its contractors (and sub-contractors) are complying with the TCPA, it should be held vicariously liable for TCPA violations committed by the telemarketer on their behalf. If the seller is not liable, it will have no incentive to ensure that prior express written consent is collected for each individual called. Allowing sellers to escape liability with a simple contract provision and no effective oversight role undermines the TCPA's purposes, which is why the FCC has taken the opposite approach.

According to the FCC, the seller "is in the best position to monitor and police TCPA compliance by third-party telemarketers," and potential liability for companies that employ third parties to robocall on their behalf "will give [the companies] appropriate incentives to ensure that their telemarketers comply with our rules." *In re Joint Petition Filed by Dish Network, LLC*, 28 F.C.C. Rcd. 6574, 6588 (2013) [hereinafter FCC DISH Order].

In contrast, allowing companies to contract out of TCPA liability would promote policies that are antithetical to the TCPA. The TCPA

incentivizes development of compliance systems to track consent and, thus, promotes knowledge of how leads are acquired. But without vicarious liability, sellers would take a hands-off approach to compliance and claim ignorance of their contractors' (and sub-contractors') practices. Unsurprisingly, this would promote ignorance and disincentivize companies from adopting strong compliance and oversight mechanisms. Any standard for vicarious liability under the TCPA should encourage more knowledge and control over compliance, not less. See FCC DISH Order at 6593 (noting that a “seller has the ability, through its authorization, to oversee the conduct of its telemarketers, even if that power to supervise is unexercised”).

A standard that fails to impose vicarious liability on companies that do not supervise their third-party telemarketers would also leave victims of illegal telemarketing without an effective remedy. FCC DISH Order at 6588. As the FCC has previously explained, third-party contractors are likely to be “judgment proof, unidentifiable, or located outside the United States, as is often the case.” *Id.* And even when a contractor can be hauled into court, enforcement against them would have little effect on the future behavior of sellers or the industry.

Without vicarious liability, sellers would just seek out another source for their insatiable appetite for leads. Indeed, because “[s]ellers may have thousands of ‘independent’ marketers, . . . suing one or a few of them is unlikely to make a substantive difference for consumer privacy.” FCC DISH Order at 6588. Attempting to shut down the web publishers and foreign call centers through direct litigation would be a game of whack-a-mole, with little real-world relief for consumers.

Sellers are also in the best position to choose companies that can indemnify them—and actually pay out—if they are at fault for violating the TCPA. *See* FCC DISH Order at 6591 (encouraging sellers to include indemnification clauses in their contracts). Placing the burden on the sellers to seek indemnification would also incentivize them to know their supply chain and to stop using disreputable contractors. *See id.* (sellers should “have an incentive to carefully choose their telemarketers to ensure compliance and to force consistent violators out of the marketplace.”) And if a contractor cannot be hauled into court or pay its part of the penalty, then the seller, who chose to engage in the risky behavior of using the third party to generate their leads and

market on their behalf, should bear the whole penalty—not the people who were harmed by behavior the seller set in motion.

Congress and the FCC have long emphasized that strong enforcement of the TCPA is essential to accomplish its purpose, and any interpretation of liability under the TCPA must ensure effective enforcement. Vicarious liability for companies like Royal Seas Cruises is the only way to accomplish this goal.

CONCLUSION

For the foregoing reasons, *amici* respectfully urge the Court to reverse the district court’s grant of summary judgment in favor of Defendant.

Date: August 9, 2021

/s/ Alan Butler

Alan Butler

Megan Iorio

ELECTRONIC PRIVACY
INFORMATION CENTER

1519 New Hampshire Ave. NW

Washington, DC 20036

(202) 483-1140

Attorneys for Amici Curiae

*Electronic Privacy Information Center
and National Consumer Law Center*

CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

This brief contains 6524 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief (*select only one*):

complies with the word limit of Cir. R. 32-1.

is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

complies with the longer length limit permitted by Cir. R. 32-2(b) because (*select only one*):

it is a joint brief submitted by separately represented parties;

a party or parties are filing a single brief in response to multiple briefs; or

a party or parties are filing a single brief in response to a longer joint brief.

complies with the length limit designated by court order dated _____.

is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature: /s/ Alan Butler

Date: August 9, 2021

CERTIFICATE OF SERVICE

I certify that on August 9, 2021, this brief was e-filed through the CM/ECF System of the U.S. Court of Appeals for the Ninth Circuit. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Date: August 9, 2021

/s/ Alan Butler

Alan Butler

Megan Iorio

ELECTRONIC PRIVACY
INFORMATION CENTER

1519 New Hampshire Ave. NW

Washington, DC 20036

(202) 483-1140

Attorneys for Amici Curiae

Electronic Privacy Information Center

and National Consumer Law Center