Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	File No.: EB-TCD-18-00027781
John C. Spiller; Jakob A. Mears; Rising Eagle	)	NAL/Acct. No.: 202032170007
Capital Group LLC; JSquared Telecom LLC;	)	FRN: 0029650744; 0029650785
Only Web Leads LLC; Rising Phoenix Group;	)	
Rising Phoenix Holdings; RPG Leads; and	)	
Rising Eagle Capital Group – Cayman	)	

NOTICE OF APPARENT LIABILITY FOR FORFEITURE

Adopted: June 9, 2020 **Released: June 10, 2020**

By the Commission: Chairman Pai and Commissioners Carr, Rosenworcel, and Starks issuing separate statements.

I. INTRODUCTION

1. This Notice of Apparent Liability proposes the largest fine in FCC history. John C. Spiller and Jakob A. Mears, doing business under the names Rising Eagle Capital Group LLC, JSquared Telecom LLC, Only Web Leads LLC, Rising Phoenix Group, Rising Phoenix Holdings, RPG Leads, and Rising Eagle Capital Group – Cayman (collectively, Rising Eagle),[1] made approximately one billion spoofed robocalls in the first four-and-a-half months of 2019 with the intent to defraud, cause harm, and wrongfully obtain something of value in apparent violation of the Truth in Caller ID Act. Given the egregious circumstances and the scope and scale of the robocall campaigns, we propose a forfeiture of $225,000,000.

II. BACKGROUND

2. *Legal Framework.* Congress recognized that consumers have long embraced caller ID as a vital part of voice telephone service, depending on it to help them decide whether to answer the phone. Caller ID is only valuable, however, if it is accurate.[2] The Truth in Caller ID Act prohibits "caus[ing] any caller identification service" in connection with any telecommunications service or Internet Protocol-enabled service to "knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value[.]"[3]

3. Spoofing on a large scale is often coupled with illegal robocalling activity. In enacting the Telephone Consumer Protection Act (TCPA), Congress determined that unwanted prerecorded voice message calls are a greater nuisance and invasion of privacy than live calls and that such calls delivered

[1] Any entity that is a "Small Business Concern" as defined in the Small Business Act (Pub. L. 85-536, as amended) may avail itself of rights set forth in that Act, including rights set forth in 15 U.S.C. § 657, "Oversight of Regulatory Enforcement," in addition to other rights set forth herein.

[2] 156 Cong. Rec. H2522, H2524 (2010) (Remarks of Rep. Engel) ("Now, if you see a caller ID and you see it has a phone number, most people think that it's ironclad that that's the actual phone number that's calling them when in truth it's not."); 155 Cong. Rec. S170-02, S173 (2009) (Remarks of Sen. Nelson) ("Consumers expect caller I.D. to be accurate because it helps them decide whether to answer a phone call and trust the person on the other end of the line.").

[3] 47 U.S.C. § 227(e); *see also* 47 CFR § 64.1604. There are exceptions for investigative, protective, or intelligence activities, but those exceptions do not apply here.

via wireless phones can be costly.[4] Through the TCPA, Congress provided greater protections for consumers from such calls.[5] The statute and the Federal Communications Commission's (Commission's or FCC's) implementing rules prohibit prerecorded voice message calls to wireless telephone numbers without subscribers' prior consent—unless they are made for an emergency purpose.[6] Telemarketing calls are also prohibited to residential numbers listed on the National Do Not Call Registry.[7] In addition, calls with artificial or prerecorded voice messages must identify, at the beginning of the message, the entity responsible for initiating the prerecorded voice message call.[8] During or after the artificial or prerecorded message, the caller must provide a telephone number, which, for telemarketing calls, the called party can dial to make a do-not-call request.[9]

4. Congress recently passed the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), which gave the Commission additional tools to pursue aggressively people who violate the laws involving illegal robocalls and caller ID spoofing.[10] The Commission has found that spoofing, when employed to further an unlawful robocalling campaign, can indicate an intent to cause harm.[11]

5. *Factual Background.* Rising Eagle made robocalls on behalf of clients that sell short-term, limited-duration health insurance plans. The largest client, Health Advisors of America, was sued by the Missouri Attorney General for telemarketing violations in February 2019. The prerecorded messages falsely implied that Rising Eagle and/or its clients were associated with well-known American health insurance companies like Blue Cross Blue Shield and Cigna. A significant portion of those calls, if not all, apparently included false or misleading caller ID information (spoofing) in a manner that violated the Truth in Caller ID Act.[12] Mr. Spiller admitted to the USTelecom Industry Traceback Group (Traceback Group) that he was making millions of calls per day, and that he was using spoofed numbers. He also admitted that Rising Eagle took affirmative steps so that the calls would go to consumers who

[4] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 18 FCC Rcd 14014, 14115, para. 165 (2003) (*2003 TCPA Order*); *Mims v. Arrow Financial Services, LLC*, 565 U.S. 368, 372 (2012) (recognizing Congress' finding that robocalls are an invasion of privacy). Courts have recognized that preserving the sanctity of the home is an important value, *see Frisby v. Schultz*, 487 U.S. 474, 484 (1988), and have found that invasion of privacy confers Article III standing in TCPA cases. *See, e.g.*, *Van Patten v. Vertical Fitness Group, LLC*, 847 F.3d 1037, 1043 (9th Cir. 2017); *LaVigne v. First Community Bancshares, Inc.*, 215 F. Supp. 3d 1138, 1146-47 (D. NM 2016).

[5] 47 U.S.C. §§ 227(b), (d)(3).

[6] 47 U.S.C. § 227(b)(1)(A)(iii); 47 CFR § 64.1200(a)(1)(iii).

[7] 47 U.S.C. § 227(c); 47 CFR § 64.1200(c)(2).

[8] 47 U.S.C. § 227(d)(3)(A); 47 CFR § 64.1200(b)(1).

[9] 47 U.S.C. § 277(d)(3)(A); 47 CFR § 64.1200(b)(2).

[10] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133 Stat. 3274 (2019) (codified as amended in 47 U.S.C. § 227) (TRACED Act). We are not pursuing TCPA violations in this enforcement action as the identified violations occurred prior to adoption of the TRACED Act.

[11] *Best Insurance Contracts, Inc., and Philip Roesel, dba Wilmington Insurance Quotes*, Forfeiture Order, 33 FCC Rcd 9204, 9218-19, paras. 40-41 (2018) (*Roesel Forfeiture Order*); *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, Forfeiture Order, 33 FCC Rcd 4663, 4668, para. 15 (2017) (*Abramovich Forfeiture Order*); *Best Insurance Contracts, Inc., and Philip Roesel, dba Wilmington Insurance Quotes*, Notice of Apparent Liability for Forfeiture, 32 FCC Rcd 6403, 6408, para. 16 (2017) (*Roesel Notice of Apparent Liability*); *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, Notice of Apparent Liability for Forfeiture, 32 FCC Rcd 5418, 5423, para. 16 (2017) (*Abramovich Notice of Apparent Liability*).

[12] Truth in Caller ID Act of 2009, Pub. L. No. 111-331, codified at 47 U.S.C. § 227(e).

had put their names on the National Do Not Call Registry,[13] because calls to those consumers enhanced his business.

6. Beginning in 2018, carriers and government enforcement personnel identified a significant trend in the number of apparently illegal prerecorded voice message calls (i.e., robocalls) on a specific subject: health insurance. Consumers across the United States increasingly complained that they were receiving robocalls selling health insurance plans and related health care products. The FCC received nearly 10,000 complaints about health insurance robocalls in 2018 and approximately 12,500 complaints about such robocalls in 2019.

7. In September 2018, the Traceback Group informed the Enforcement Bureau (Bureau) that it had traceback information for millions of robocalls containing prerecorded messages about health insurance.[14] The Traceback Group determined that approximately 23.6 million health insurance robocalls were crossing the networks of the four largest wireless carriers each day.[15] Moreover, the Traceback Group's experts found indications that many or possibly all of the offending robocalls contained false caller ID information. The Bureau launched a formal investigation to determine who was responsible for the apparently unlawful spoofed robocalls affecting consumers.

8. These robocalls also attracted the attention of media outlets and consumer protection advocates. The *Philadelphia Inquirer* reported in November 2018 that prerecorded calls offering health insurance plans topped the list of problematic robocalls.[16] State insurance regulators likewise warned consumers not to be fooled by robocalls making misleading claims about the quality or scope of coverage of the health insurance plans that the recorded messages were marketing.[17] Meanwhile, consumers filed complaints with the Commission and the Federal Trade Commission about the offending robocalls they received.

9. The Bureau uncovered evidence that many of the robocalls at issue here included false or misleading statements about the identity of the caller and the products being offered. The messages purported to offer health insurance plans from well-known health insurance companies such as Aetna, Blue Cross Blue Shield,[18] Cigna, and UnitedHealth Group. For example, some calls included the following message:

---

[13] Federal Trade Commission, National Do Not Call Registry, https://www.donotcall.gov/.

[14] Letter from Kevin G. Rupy, Vice President, Law & Policy, USTelecom—The Broadband Association, to Kristi Thompson, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Sept. 21, 2018) (on file in EB-TCD-18-00027781). Traceback is the process of tracing suspected illegal robocalls through multiple voice service provider networks until the originating voice provider or the calling party is identified. USTelecom Industry Traceback Group, 2019 Progress Report at 3 (2019), https://www.ustelecom.org/wp-content/uploads/2020/01/ITG-2019-Progress-Report.pdf.

[15] USTelecom Subpoena Response (Oct. 4, 2018) (on file in EB-TCD-18-00027781).

[16] Christian Hetrick, *The Most Rampant Robocall Scams Are Linked to Health Insurance, Amazon and Student Loans,* The Philadelphia Inquirer (Nov. 15, 2018), https://www.inquirer.com/philly/business/consumer_news/robocall-scams-amazon-spoofing-health-insurance-blocker-20181115.html.

[17] *See* Nevada Division of Insurance, *Consumer Alert: Division Warns Consumers of Telemarketers Deceiving Discount Plans as Comprehensive Health Insurance,* (Nov. 21, 2018), http://doi.nv.gov/News_Notices/Press_Releases/Consumer_Alert__Division_warns_consumers_of_telemarketers_deceiving_discount_plans_as_comprehensive_health_insurance/.

[18] Blue Cross Blue Shield is comprised of 36 independent and locally operated companies. Together these companies form the Blue Cross Blue Shield Association, which owns the intellectual property rights. *The Blue Cross Blue Shield System*, Blue Cross Blue Shield, https://www.bcbs.com/about-us/the-blue-cross-blue-shield-system (last visited Feb. 20, 2020). References to Blue Cross Blue Shield in this Notice of Apparent Liability are to the Blue Cross Blue Shield system as a whole.

> Are you looking for affordable health insurance with benefits from a company you know? Policies have all been reduced nationwide such as Cigna, Blue Cross, Aetna, and United[,] just a quick phone call away. Press 3 to get connected to a licensed agent or press 7 to be added to the Do Not Call list.[19]

Contrary to the message, however, if a consumer "press[ed] 3" after hearing the message, he or she would be transferred to a call center unaffiliated with and not authorized by the named companies.[20] The representatives in that call center then would attempt to convince the caller to purchase an insurance product sold by one of Rising Eagle's clients.

10. The Bureau confirmed that at least two of the insurance companies mentioned in the prerecorded voice messages had nothing to do with the robocalls. Blue Cross Blue Shield and Cigna provided affidavits to the Bureau asserting that neither company made any such calls.[21] In fact, Cigna does not even offer the type of health insurance being offered in the robocalls.[22] Blue Cross Blue Shield told Bureau investigators that the robocalls caused significant harm to the company. Blue Cross Blue Shield reported that it has been sued multiple times by plaintiffs' attorneys seeking damages under the TCPA's private right of action, incurring direct financial harm as a result of the robocalls that falsely invoked the Blue Cross Blue Shield name.[23] Blue Cross Blue Shield also stated that it received many complaints from robocall victims. Consumers expressed a great deal of anger and frustration about the calls, which they believed were associated with Blue Cross Blue Shield. One consumer, for example, complained:

> I am so tired of receiving robo calls up to ten a day from Blue Cross that I am pressing our company to drop you. Reaching out to my congressmen to some how [sic] fine you and expose you. OMG I just took another while writing this . . . [orig.] I hope tens of thousands of people start complaining about you as I am about to make this a personal goal to have your company fined for every call made and yes I am on the do not call list.[24]

11. The Bureau determined that Rising Eagle Capital Group, LLC was apparently responsible for the robocalls impersonating Blue Cross Blue Shield and Cigna on behalf of Health Advisors and

---

[19] Nomorobo, *(678) 261-1817 Is a Health Insurance Scam* (Feb. 6, 2019), https://www nomorobo.com/lookup/678-261-1817.

[20] One of the call centers to which consumers were routed on the calls at issue here was Health Advisors of America, Inc., run by Michael Smith Jr. and Zachary Cox in Florida (collectively Health Advisors). The Missouri Attorney General sued Health Advisors for telemarketing violations in February 2019. *Missouri v. Health Advisors of America, Inc. et al.,* Petition for Permanent Injunction, Civil Penalties, and Other Relief, 19SL-CC00580 (Feb. 8, 2019). The Missouri Attorney General reached a settlement on August 8, 2019. *Missouri v. Health Advisors of America, Inc. et al.*, Consent Judgment, 19SL-CC00580 (Aug. 8, 2019). Similarly, the Florida Department of Agriculture and Consumer Services sued Health Advisors for telemarketing violations in May 2019. *Dept. of Agriculture and Consumer Services v. America's Best Insurance Group, Inc.*, Final Order, 1809-41258 (May 8, 2019). Health Advisors was not authorized to sell any products offered by the companies mentioned in the robocalls. Affidavit of Kaitlin Reilly, Legal Compliance Senior Advisor, Cigna Corporation at 1-2 (Feb. 12, 2020) (Cigna Aff.); Affidavit of Adam Peltzman, Assistant General Counsel, Executive Director, Blue Cross Blue Shield Association at 1 (Apr. 10, 2020) (Blue Cross Aff.).

[21] Cigna Aff. at 1-2; Blue Cross Aff. at 1-2.

[22] Cigna Aff. at 2. Centers for Medicare & Medicaid Services, Fact Sheet, Short-Term, Limited-Duration Insurance Final Rule (Aug. 1, 2018), https://www.cms.gov/newsroom/fact-sheets/short-term-limited-duration-insurance-final-rule.

[23] Unlawful spoofed robocalls such as those initiated by Rising Eagle can lead to TCPA litigation. *See* Blue Cross Aff. at 2, Attach. A.

[24] *See e.g.*, Blue Cross Aff. at 2, Attach. B.

others. The Traceback Group's efforts identified R Squared Telecom LLC, an Ohio VoIP provider, as the originating provider of the robocalls.[25] The Bureau subpoenaed R Squared for information about the robocalls, and R Squared identified Rising Eagle Capital Group, LLC as the originator of the robocalls.[26] Rising Eagle Capital Group, LLC is a Texas company controlled by John Spiller and his business partner, Jakob Mears.[27] Mr. Spiller and Mr. Mears also controlled Only Web Leads LLC and JSquared Telecom LLC and conduct business as Rising Phoenix Group and RPG Leads.[28] Together these businesses were vehicles for Mr. Spiller and Mr. Mears to make millions of lead generation calls each day for various clients offering health care products.

12. Between January 2, 2019 and May 14, 2019, Rising Eagle made 1,047,677,198 robocalls to American and Canadian consumers.[29] These robocalls were extremely disruptive to consumers' lives, according to the victims:

- I am disabled and elderly. I continue to receive repeated calls from this same caller. They call 2 - 3 times per day. I sometimes fall when trying to get to the phone. This caller sells Cigna, BlueCross/Blue Shield health care plans and others. It's recorded. Can't hardly take it anymore. Can't get my rest.[30]
- I took my phone off the hook for 3 days because I didn't want to here [sic] their annoying calls anymore, otherwise I would have had twice this amount of disgusting numbers. If they were a legit business why would they be changing their phone number and ID, with the same message, all the time?[31]
- I have requested at least 15 times to be placed on a do not call list. I get relentless calls, maybe 15-20 a day from masked numbers. I've reported many of them to the DNC registry, but it hasn't even slowed down let alone stopped.[32]

13. Additionally, these robocalls disrupted the consumers and businesses whose numbers were spoofed by Rising Eagle. For example, Genworth North America Corporation (Genworth), a long-term care and life insurance company, was spoofed nearly 10 million times.[33] Genworth's telephone

[25] USTelecom Subpoena Response (Oct. 4, 2018) (on file in EB-TCD-18-00027781).

[26] R Squared Subpoena Response (May 31, 2019) (on file in EB-TCD-18-00027781).

[27] Rising Eagle Capital Group LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Apr. 9, 2014); Rising Eagle Capital Group LLC, Certificate of Amendment, Office of the Sec'y of State of Tex. (June 1, 2018) (adding Jakob Mears as a member and director).

[28] Only Web Leads LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Nov. 20, 2018); JSquared Telecom LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Jan. 30, 2019); Rising Eagle Capital Group LLC, Assumed Name Certificate, Office of the Sec'y of State of Tex. (Jan. 12, 2015) (creating the assumed name of Rising Phoenix Holdings); Rising Eagle Capital Group LLC, Assumed Name Certificate, Office of the Sec'y of State of Tex. (Mar. 17, 2017) (creating the assumed name of RPG Leads).

[29] R Squared Subpoena Response (Aug. 16, 2019) (on file in EB-TCD-18-00027781) (Call Detail Records). Rising Eagle made 2,672,424 robocalls to Canadian consumers; however, the 150,000 robocalls verified by the Bureau only include robocalls made to U.S. consumers. The Truth in Caller ID Act prohibits unlawfully spoofed calls to U.S. *and* foreign recipients so long as the caller is located in the United States. 47 U.S.C. § 227(e). Rising Eagle is a Texas entity. Rising Eagle Capital Group LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Apr. 9, 2014).

[30] FCC Complaint #3070502 (Feb. 21, 2019).

[31] FCC Complaint #3060950 (Feb. 18, 2019).

[32] FCC Complaint #3188235 (Apr. 12, 2019).

[33] Call Detail Records.

network became unusable because it was inundated with so many callbacks from angry consumers.[34] Consumers also thought Genworth was responsible for the robocalls and left angry messages with the company.[35]

14. The Bureau reviewed a sample of Rising Eagle's more than one billion robocalls for violations of the Act. Bureau staff verified that Rising Eagle used at least 60 caller IDs assigned to persons other than Rising Eagle or that were unassigned. We also verified that many of the robocalls went to numbers listed on the national Do Not Call Registry.[36] Rising Eagle called many consumers multiple times—sometimes several hundred times over the four-and-half-month period and nearly a dozen times a day.[37] Additionally, the Bureau analyzed these robocalls using an industry-standard, commercially available software and database of known assigned and ported wireless numbers to determine whether any of the robocalls went to wireless phones.[38] Bureau staff confirmed that Rising Eagle made at least 86,864,456 robocalls to wireless phones as well as 56,635,935 robocalls to numbers listed on the National Do Not Call Registry. Finally, the recordings connected to the robocalls examined by Bureau staff contained neither the name of the caller at the beginning of the prerecorded voice message nor a callback telephone number.[39]

15. Bureau staff spoke with 52 consumers who received robocalls from Rising Eagle. None of the consumers who the Bureau contacted gave permission—written or otherwise—to Rising Eagle to make robocalls to their phones.[40] Neither did these complainants give Rising Eagle consent to make telemarketing robocalls.

16. On multiple occasions over the course of 2019, the Traceback Group notified Rising Eagle that its calling campaigns were illegal. The Traceback Group sent traceback notices to Mr. Spiller informing him that his calls had generated numerous complaints by recipients and warning that his calls appeared to violate federal laws against unsolicited telemarketing robocalls and malicious spoofing. A consultant with the Traceback Group contacted Mr. Spiller about the robocalls on June 7, 2019.[41] Mr. Spiller admitted to the consultant that he made millions of robocalls daily.[42] He informed the consultant that he had just stopped using spoofed numbers in June 2019. He thus admitted that he was using spoofed

[34] Affidavit of Matthew J. Klaus, Chief Information Security Officer, Genworth North America Corporation at 1-2 (Mar. 16, 2020) (Genworth Aff.). Consumers also left complaints on Genworth's social media accounts. *Id.* at 2.

[35] Genworth Aff. at 1.

[36] Call Detail Records.

[37] *Id.*

[38] *See* Interactive Marketing Solutions, EasyID, https://www.ims-dm.com/mvc/page/easyid/ (last visited May 3, 2020). EasyID is Interactive Marketing Solutions' software that allows clients to eliminate wireless numbers from calling lists. *Id*. Interactive Marketing Solutions, Inc. is a member of the Direct Marketing Association and bills itself as "the country's largest single-source supplier" of data identifying telephone numbers that have been assigned or ported to wireless devices, "to help businesses comply with state and federal legislation." Interactive Marketing Solutions – Do Not Contact List Solutions, https://www.ims-dm.com/mvc/index.php (last visited May 3, 2020).

[39] Bureau staff examined recordings provided by YouMail, a robocall identification and blocking service. YouMail Subpoena Response (Jan. 3, 2020) (on file in EB-TCD-18-00027781) (YouMail Response).

[40] Declaration of {[ ]} (Apr. 8, 2020) (on file in EB-TCD-18-00027781); Declaration of {[}] (Apr. 6, 2020) (on file in EB-TCD-18-00027781); Declaration of {]} (Mar. 12, 2020) (on file in EB-TCD-18-00027781); Declaration of {[ ]} (Mar. 10, 2020) (on file in EB-TCD-18-00027781); Declaration of {[ ]} (Mar. 9, 2020) (on file in EB-TCD-18-00027781). Material highlighted and set off by double brackets {[ ]} is redacted from the public version of this document.

[41] Affidavit of David Frankel at 2 (Jan. 9, 2020) (Frankel Aff.).

[42] *Id.*

caller ID until after the calls at issue in this Notice of Apparent Liability.[43] He further admitted that he had disabled the function of his calling platform that prevented robocalls from going to numbers registered on the National Do Not Call Registry. According to Mr. Spiller, he started making telemarketing robocalls to consumers who put their numbers on the Do-Not-Call List because he "found that his sales rates . . . rose substantially" when he did so.[44] The Traceback Group continued to send traceback notices to Rising Eagle throughout 2019.[45] Mr. Spiller informed the Traceback Group that he ceased spoofing caller ID on September 10, 2019.[46] Rising Eagle, however, continued to make telemarketing robocalls.[47]

III. DISCUSSION

17. The Bureau's investigation indicates that Rising Eagle's activities appear to have violated the Truth in Caller ID Act. It is unlawful to display misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value.[48] Our investigation determined that Rising Eagle apparently used approximately 170,000 unique caller IDs to make 1,047,677,198 calls. None of these phone numbers apparently were assigned to Rising Eagle. Caller ID information is spoofed when it is manipulated or altered to display anything other than the originating telephone number. Spoofing is unlawful under the Truth in Caller ID Act when it is done with the intent to defraud, cause harm, or wrongfully obtain anything of value.[49]

18. With respect to robocalls at issue here, Rising Eagle apparently knowingly displayed misleading or inaccurate caller ID information with all three forms of unlawful intent:

> *Intent to Defraud*: Evidence shows that Rising Eagle apparently intended to defraud consumers by deceiving them into thinking that the robocalls were made by or on behalf of major health insurance brands in order to induce consumers to purchase insurance products from companies other than the brands identified.
>
> *Intent to Cause Harm*: Rising Eagle apparently intended to cause harm to the goodwill of major health insurance brands by associating those brands with a nationwide campaign of illegal robocalls. Rising Eagle also apparently intended to harm consumers it called by making large numbers of unlawful telemarketing robocalls in violation of the TCPA. Rising Eagle also apparently intended to harm the true subscribers of the numbers that Rising Eagle spoofed, as well as the telephone carriers that had to use significant time and resources to manage the robocalls and contend with the public outrage from the calls.
>
> *Intent to Wrongfully Obtain Anything of Value*: Rising Eagle apparently intended to wrongfully obtain something of value. Specifically, Rising Eagle used spoofed caller ID in connection with unlawful robocalls to sell insurance products and to evade liability from individuals exerting their private right of action and from government enforcement. In addition, Rising Eagle apparently intended to make the spoofed robocalls to consumers who were on the National Do Not Call Registry specifically to increase its sales rates.

---

[43] *Id.*

[44] *Id.*

[45] *Id.* at 3-5.

[46] *Id.* at 3-4.

[47] The Traceback Group continued to identify Spiller in tracebacks throughout 2019. *See* Frankel Aff. at 2-4. This NAL does not include robocalls made after May 14, 2019 and is without prejudice to any future enforcement action with respect to them.

[48] 47 U.S.C. § 227(e); 47 CFR § 64.1604.

[49] 47 U.S.C. § 227(e); 47 CFR § 64.1604.

We thus determine that Rising Eagle is apparently liable for violation of section 227(e) of the Act and section 64.1604 of the Commission's rules.

19. We propose a forfeiture in the amount of $225,000,000. We calculate the proposed forfeiture by assessing a base forfeiture of $1,000 per each apparently unlawful call. As we have in other mass-spoofing cases, we analyze and verify a portion of the apparently unlawfully spoofed calls and apply the proposed forfeiture amount to those verified calls. In this case, staff verified 150,000 apparently unlawful spoofed calls, yielding a base forfeiture of $150,000,000. We then apply an upward adjustment to the proposed amount to reflect the nature, circumstances, extent, and gravity of the apparent violations for which Rising Eagle is highly culpable.

A. Rising Eagle Apparently Knew That It Was Using Inaccurate Caller ID Information.

20. The Truth in Caller ID Act prohibits a caller from knowingly transmitting misleading or inaccurate caller ID information with the requisite intent. Of the 60 distinct telephone numbers that Rising Eagle spoofed, not one was assigned to Rising Eagle. The numbers were assigned to an unrelated third party or were unassigned. Moreover, Rising Eagle apparently knew that between January 2, 2019 and May 14, 2019 it was using numbers that it did not have the right to use. In June 2019, Mr. Spiller told a Traceback Group consultant that Rising Eagle *had started* acquiring numbers to use as caller IDs—indicating that Rising Eagle knew that prior to that time, it had been using inaccurate caller ID information. On September 10, 2019, Mr. Spiller admitted to the Traceback Group consultant that "we just started the new process of not using spoofed numbers on September 10th at 11am EST . . . So yes on the 9th we were still using the old way of using spoofed numbers."[50] Thus, Rising Eagle apparently knowingly transmitted misleading or inaccurate caller ID.

B. Rising Eagle Apparently Intended to Defraud, Cause Harm, and Wrongfully Obtain Something of Value.

1. Rising Eagle Apparently Intended to Defraud Consumers into Thinking that They Were Being Offered Health Insurance Products from Well-Known Health Insurance Brands.

21. The Truth in Caller ID Act and the Commission's rules prohibit knowingly displaying misleading or inaccurate caller ID information with the intent to defraud.[51] We look to other Commission and court decisions to determine the meaning of the term "defraud" in the context of the Truth in Caller ID Act. The Commission has previously addressed fraud in the context of the federal wire fraud statute finding that a fraudulent scheme "is a plan to deceive persons as to the substantial identity of the things they are to receive in exchange."[52] Similarly, common law fraud consists of the following elements: "(1) a false representation (2) in reference to a material fact (3) made with knowledge of its falsity (4) and with the intent to deceive (5) with action taken in reliance upon the representation."[53] The wrongdoer must know that the representation was false or have asserted the representation without knowledge of its truth.[54] The factual false representation is material "if it would likely affect the conduct of a reasonable

[50] Frankel Aff. at 3.

[51] 47 U.S.C. § 227(e); 47 CFR § 64.1604.

[52] *Network Services Solutions, LLC, Scott Madison*, Notice of Apparent Liability for Forfeiture and Order, 31 FCC Rcd 12238, 12276, para. 112 (2016).

[53] *Pence v. United States*, 316 U.S. 332, 338 (1942); *see also Zorrilla v. Aypco Constr. II, LLC*, 469 S.W.3d 143, 153 (Tex. 2015) ("[A] material misrepresentation, which was false, and which was either known to be false when made or was asserted without knowledge of its truth, which was intended to be acted upon, which was relied upon, and which caused injury.").

[54] *Johnson & Higgins of Texas, Inc. v. Kenneco Energy, Inc.*, 962 S.W.2d 507, 527 (Tex. 1998).

person concerning the transaction."[55] Intent can be inferred from the totality of the circumstances rather than direct evidence.[56] Several factors can be considered to determine intent: (1) whether the wrongdoer acted with reckless disregard for the truth;[57] (2) whether the wrongdoer avoided knowledge of the scheme;[58] (3) whether the wrongdoer made affirmative misrepresentations by statements, acts, or omissions;[59] or (4) whether the victim relied on those misrepresentations.[60] Finally, common law fraud requires actual and justified reliance by the victim.[61] The Truth in Caller ID Act, however, only requires a showing of *intent* to defraud rather than actual reliance and harm.

22. Rising Eagle made material, affirmative misrepresentations in spoofed prerecorded voice message calls. These misrepresentations created a false impression that the robocalls were made by, or were otherwise affiliated with, specific health insurance companies when that was not the case. Rising Eagle apparently falsely represented that the called party was receiving an offer to purchase health insurance from a well-known company such as Blue Cross Blue Shield and Cigna. This misrepresentation was critical to inducing consumers to "press 3" and listen to the sales pitches of its call center clients. Furthermore, the spoofing made it more likely that consumers would answer the phone and listen to the fraudulent sales pitch. *First*, because the calls were spoofed, consumers could not accurately identify the caller. *Second*, because Rising Eagle relied on a large array of spoofed numbers, consumers could not readily correlate the caller ID to Rising Eagle and choose to ignore or block the future calls from the company.[62] Once consumers reached the call center, they would be presented with a variety of offers from providers of short-term, limited-duration health insurance plans rather than the long-term coverage for which the mentioned companies are known; neither Rising Eagle nor Rising Eagle's clients were authorized to sell those companies' products.[63] In fact, some of the mentioned insurance companies,

[55] *In re Primera Energy, LLC*, 579 B.R. 75, 145 (Bankr. W.D. Tex. 2017), *aff'd sub nom*; *Custom Leasing, Inc. v. Texas Bank & Trust Co. of Dallas*, 516 S.W.2d 138, 142 (Texas 1974).

[56] *See United States v. O'Connell*, 172 F.3d 921 (D.C. Cir. 1998); *see also United States v. Alston*, 609 F.2d 531, 538 (D.C. Cir. 1979), *cert. denied,* 445 U.S. 918 (1980). Specific intent does not require that the wrongdoer intended to violate the law. *United States v. Bibby*, 752 F.2d 1116, 1124 (6th Cir. 1985).

[57] *United States v. Cusino*, 694 F.2d 185, 187 (9th Cir. 1982), *cert. denied,* 461 U.S. 932 (1983).

[58] *United States v. Ramsey*, 785 F.2d 184 (7th Cir. 1986), *cert. denied,* 476 U.S. 1186, 1189 (1986).

[59] *See Cusino*, 694 F.2d at 187.

[60] *United States v. Ranney*, 719 F.2d 1183, 1188-89 (1st Cir. 1983) (citing *Phillips v. United States*, 356 F.2d 297, 308 (9th Cir. 1965)).

[61] *Grant Thornton LLP v. Prospect High Income Fund*, 314 S.W.3d 913, 923 (Tex. 2010).

[62] Consumers may ask providers to block specific phone numbers, a process called "blacklisting." By using many different spoofed numbers, Rising Eagle made blacklisting ineffective.

[63] Neither Cigna nor Blue Cross Blue Shield authorized Rising Eagle's largest client, Health Advisors, to sell their products. Cigna Aff. at 1-2; Blue Cross Aff. at 1. Michael T. Smith, Jr., P112070, Licensee Detail, Florida Department of Financial Services, https://licenseesearch fldfs.com/Licensee/933080 (last visited Feb. 18, 2020); Zachary Cox, W413251, Licensee Detail, Florida Department of Financial Services, https://licenseesearch.fldfs.com/Licensee/1661313 (last visited Feb. 18, 2020). Instead, Health Advisors sold health insurance through Health Insurance Innovations, Inc. (HII), an online distributor of short-term, limited-duration health plans. Health Insurance Innovations, Inc., Annual Report (Form 10-K) (Mar. 14, 2019) (HII 10-K); *see also* Zeke Faux, Polly Mosendz, and John Tozzi, *Health Insurance That Doesn't Cover the Bills Has Flooded the Market Under Trump*, Bloomberg Businessweek (Sept. 17, 2019), https://www.bloomberg.com/news/features/2019-09-17/under-trump-health-insurance-with-less-coverage-floods-market (noting HII's central role in the short-term, limited-duration health market). HII admits in filings with the Securities Exchange Commission that its third-party distributors engage in telemarketing to sell HII products. *See* HII 10-K. In some cases, HII provides advanced commission arrangements to its third-party distributors to assist with the cost of lead acquisition. *Id.* Zachary Cox entered such a financing arrangement with HII on January 8, 2018. *See* Doc. No. 201803963148, Florida Secured Transaction Registry (Jan. 25, 2018),

(continued….)

such as Cigna, do not even offer short-term, limited-duration health insurance plans.[64] Blue Cross Blue Shield, meanwhile, does not interact with consumers using the name "Blue Cross;" rather, its independent, regional operating companies must use their corporate or trade names such as CareFirst.[65] Rising Eagle was not authorized to sell Blue Cross Blue Shield or Cigna products nor did it have any reasonable belief that its clients had such authorization. Rising Eagle apparently intentionally made these misrepresentations of specific, well-known insurance providers because the misrepresentations increased the likelihood that a consumer would "press 3" to be transferred to one of Rising Eagle's clients. In return, Rising Eagle was compensated for the successful transfers.[66] Thus, we find that Rising Eagle spoofed calls with the apparent intent to defraud.

2. Rising Eagle Apparently Intended to Cause Harm to Health Insurance Companies, Subscribers of the Spoofed Numbers, Consumers, and Carriers.

23. The Truth in Caller ID Act and the Commission's rules prohibit knowingly displaying misleading or inaccurate caller ID information with the intent to cause harm.[67] The Commission has held that the element of "harm" in the Truth in Caller ID Act is broad and "encompasses financial, physical, and emotional harm . . . ."[68] Moreover, the Commission has established that an intent to harm under the Truth in Caller ID Act can be demonstrated when the harms are "consequences which are desired" or "substantially certain."[69] Courts have recognized that direct evidence of specific intent is rarely available.[70] Therefore, it is reasonable and often necessary to look at a party's actions to determine the party's intent regarding a wrongful action.[71] We find sufficient evidence that Rising Eagle apparently

(Continued from previous page)
https://www.floridaucc.com/uccweb/SearchResultsDetail.aspx?sst=&sov=6&sot=Document%20Number&st=201803963148&fn=201803963148&rn=1&ii=Y&ft=1&epn=.

[64] Cigna Aff. at 2.

[65] Blue Cross Blue Shield, *Healthcare Fraud*, https://www.bcbs.com/healthcare-fraud (last visited May 4, 2020).

[66] Rising Eagle Bank Records (on file in EB-TCD-18-00027781).

[67] 47 U.S.C. § 227(e); 47 CFR § 64.1604.

[68] *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, Report and Order, 26 FCC Rcd 9114, 9122, para. 22 (2011) (*Truth in Caller ID Order*).

[69] *See Affordable Enterprises of Arizona, LLC*, Notice of Apparent Liability for Forfeiture, 33 FCC Rcd 9233, 9242-43, para. 26 & n.70 (2018) (*Affordable Notice of Apparent Liability*) (citing Restatement (Second) of Torts § 8A, comment b, p. 15 ("Intent is not . . . limited to consequences which are desired. If the actor knows that the consequences are certain, or substantially certain, to result from his act, and still goes ahead, he is treated by the law as if he had in fact desired to produce the result.")). *Cf. Burr v. Adam Eidemiller, Inc.*, 386 Pa. 416 (1956) (intentional invasion can occur when the actor knows that it is substantially certain to result from his conduct); *Garratt v. Dailey*, 13 Wash. 2d. 197 (1955) (finding defendant committed an intentional tort when he moved a chair if he knew with "substantial certainty" that the plaintiff was about to sit down).

[70] *United States v. Dearing*, 504 F.3d 897, 901 (9th Cir. 2007); *United States v. Marabelles*, 724 F.2d 1374, 1379 (9th Cir. 1984); *see also General Cigar Co., Inc. v. CR Carriers, Inc.*, 948 F.Supp. 1030, 1036 (M.D. Ala. 1996) ("Because one cannot know another's subjective intent, circumstantial evidence must be relied upon to indicate intent. The requirement of specific intent under the mail fraud statute is satisfied by the existence of a scheme which was reasonably calculated to deceive persons of ordinary prudence and comprehension and this intention is shown by examining the scheme itself." (internal citations omitted)).

[71] *United States v. Davis*, 490 F.3d 541, 549 (6th Cir. 2007); *Tusa v. Omaha Auto Auction Inc.*, 712 F.2d 1248, 1253 (8th Cir. 1983) ("[I]ntent to defraud is ordinarily proved by circumstantial evidence."); *see also United States v. Sullivan*, 522 F.3d 967, 974 (9th Cir. 2008) ("[T]he scheme itself may be probative circumstantial evidence of an intent to defraud."); *United States v. Rogers*, 321 F.3d 1226, 1230 (9th Cir. 2003) ("It is settled law that intent to defraud may be established by circumstantial evidence."); *General Analytics Corp. v. CNA Ins. Cos.*, 86 F.3d 51, 54 (4th Cir. 1996) ("[B]ecause it is abstract and private, intent is revealed only by its connection with words and conduct."); *FDIC v. St. Paul Fire & Marine Ins. Co.*, 942 F.2d 1032, 1035 (6th Cir. 1991) ("intent . . . is thought to
(continued….)

intended to cause harm to: (1) the goodwill of well-known health insurance companies whose reputations and brand names were used, (2) the subscribers of the telephone numbers that Rising Eagle spoofed, (3) consumers who received the calls, and (4) the terminating carriers forced to deliver large numbers of unsolicited robocalls and handle consumers' corresponding ire.

24. *Harm to Health Insurance Companies.* Rising Eagle's spoofed robocalls harmed the companies mentioned in the robocall messages. In *Adrian Abramovich*, the Commission concluded that Abramovich's robocalls using the names of well-known travel and hospitality brands severely harmed those companies and the goodwill of their brands.[72] Like Abramovich, Rising Eagle selected well-known and long-established corporate names or brands—in this case, health care insurance companies like Blue Cross Blue Shield and Cigna—to which Rising Eagle or its clients had no relationship.[73] Blue Cross Blue Shield received complaints from consumers who mistakenly thought the calls came from them.[74] Blue Cross Blue Shield posted a consumer alert on its website stating that its licensed companies do not refer to themselves as "Blue Cross."[75] Rising Eagle's robocalls also exposed the misrepresented companies to numerous TCPA class action lawsuits.[76] Rising Eagle used spoofed caller ID to increase the likelihood that consumers would answer the calls. In addition, by masking the originating number, or spoofing, consumers could not identify the perpetrators of the robocalls, and consumers would continue to associate the unwanted calls with the companies named. The longer it takes to detect the source of the calls, the more damage can be done to the companies' reputations. By using well-known corporate or brand names that Rising Eagle was not authorized to use in its massive robocalling campaigns and by spoofing the originating number of those calls, it was substantially certain that the goodwill of those brands and companies would suffer harm. Therefore, we find that Rising Eagle apparently intended to harm the companies and brands that it used in its robocalls.

25. *Harm to Users of the Spoofed Numbers.* The Commission has found that spoofing is harmful to the innocent third parties whose numbers are spoofed.[77] In *Abramovich*, the Commission recognized that people frequently redial a spoofed number to determine who called or to express outrage.[78] In *Affordable*, the Commission said:

> [A] person whose number is spoofed by a telemarketer and used to make large numbers of illegal calls often finds herself inundated with callbacks and angry messages from the

(Continued from previous page)
refer to a subjective phenomenon that takes place inside people's heads . . . . [The law is concerned only with] the external behavior ordinarily thought to manifest internal mental states . . . .") (citations omitted)).

[72] *Abramovich Forfeiture Order*, 33 FCC Rcd at 4668, para. 16.

[73] Cigna Aff. at 2; Blue Cross Aff. at 1-2. Rising Eagle's largest client, Health Advisors, had no connection to Cigna or BCBS during the period of the Bureau's investigation. Cigna Aff. at 2; Blue Cross Aff. at 1-2.

[74] Blue Cross Aff. at 2.

[75] Blue Cross Blue Shield, *Healthcare Fraud*, https://www.bcbs.com/healthcare-fraud (last visited May 4, 2020) ("Blue Cross Blue Shield Association has received reports that some individuals are receiving robocalls that falsely claim to be made by "Blue Cross Blue Shield." These calls may seek to market insurance products or collect personal information from call recipients. Neither Blue Cross Blue Shield Association nor any of the Blue Cross and Blue Shield companies licensed to use the Blue Cross® and/or Blue Shield® brands are making these calls. . . . If you get a recorded call from a caller whom you did not authorize to call you, the call is likely fraudulent or malicious and you should hang up immediately.").

[76] Blue Cross Aff. at 2.

[77] *Roesel Forfeiture Order*, 33 FCC Rcd at 9217, para. 37; *Abramovich Forfeiture Order*, 33 FCC Rcd at 4668, para. 14; *Affordable Notice of Apparent Liability*, 33 FCC Rcd at 9243, para. 28; *Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6411, para. 23; *Abramovich Notice of Apparent Liability*, 32 FCC Rcd at 5424, para. 18.

[78] *See Abramovich Notice of Apparent Liability*, 32 FCC Rcd at 5424, para. 18 (implying that even one callback from an angry consumer is a harm).

> telemarketer's other, and often irate, victims. In short, by spoofing numbers assigned to legitimate users, Affordable shifted the risk of harm—large numbers of disturbing calls from angry consumers—on to innocent third parties.[79]

It is substantially certain that such harm will occur when a spoofer knowingly uses a number that does not belong to him to make a large number of calls and instead uses a number assigned to someone else. Accordingly, the intent to cause harm may be imputed to the spoofer.[80]

26. Of the 60 spoofed caller IDs that the Bureau identified, 21 of the numbers were assigned to third parties unaffiliated with Rising Eagle. Rising Eagle apparently spoofed each number on average at least 3.7 million times.[81] For example, Rising Eagle spoofed five numbers belonging to Genworth to make 9,861,464 robocalls.[82] Angry consumers responded by calling back the spoofed numbers, which resulted in Genworth's telephone network being overwhelmed, making it inoperable for some of its employees.[83] Consumers also blamed Genworth for the robocalls. Many complained on Genworth's social media accounts to express their outrage.[84] Rising Eagle's robocalls were harmful to users of the numbers that it spoofed as well as disruptive to at least one company's operations and reputation.

27. Additionally, Rising Eagle spoofed at least 39 unassigned numbers. As the Commission held in *Roesel*, repeated use of unassigned numbers is a strong indication that the caller has the intent to defraud or cause harm.[85] Most of the unassigned numbers used by Rising Eagle were flagged by caller identification services as untrustworthy. For example, Nomorobo flagged 678-261-3311, a number that Rising Eagle spoofed 2,299,952 times, as a "Phone Scam Alert!" and "Health Insurance Scam."[86]

28. The impact associated with such flagging goes beyond the immediate beneficial goal of the scam warning, however. Any service provider that allocates the previously unassigned phone number to a subscriber in the future risks saddling that subscriber with a toxic phone number.[87] Moreover, as additional whitelist/blacklist-based call blocking tools appear in the market for consumer use, consumers who obtain toxic numbers may find themselves unable to contact other end users who have blocked the number to cut off an illegal robocaller.[88] Such misuse of unassigned numbers in this way causes harm by

---

[79] *Affordable Notice of Apparent Liability*, 33 FCC Rcd at 9243, para. 28.

[80] *See id.* at 9242-43, paras. 25-26 (discussing that intent can be inferred if the action is "substantially certain" to cause harm).

[81] Call Detail Records.

[82] *Id.*

[83] Genworth Aff. at 1-2.

[84] *Id.*

[85] *Roesel Forfeiture Order*, 33 FCC Rcd at 9215-16, para. 33, n.85; *see also Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6411, para. 23; *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706, 9713, para. 18 (2017) ("Use of an unassigned number provides a strong indication that the calling party is spoofing the Caller ID to potentially defraud and harm a voice service subscriber. Such calls are therefore highly likely to be illegal.").

[86] Nomorobo, *(678) 261-3311* (Feb. 8, 2019), https://www.nomorobo.com/lookup/678-261-3311. The number is also identified in multiple Internet forums dedicated to combatting robocalls. *See* Alex, *678-261-3311*, 800notes.com (Feb. 8, 2019), https://800notes.com/Phone.aspx/1-678-261-3311.

[87] *Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6411, para. 23.

[88] *Id*. Whitelist-based call blocking allows consumers to tell their service provider to accept calls only from specified numbers. *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876, 4890, para. 43 (2019). Blacklist-based call blocking allows service providers or call blocking applications to block incoming suspect calls based on analytics. *Id*. at 4887, para. 34.

(1) constricting the supply of quality phone numbers available for assignment, and (2) causing blocking apps potentially to over-block in an effort to give users relief from unwanted calls.[89] It was substantially certain that the unauthorized use of spoofed numbers as part of a massive robocalling campaign would result in unwanted attention to those numbers. Therefore, we find that Rising Eagle apparently intended to harm the legitimate users of the spoofed numbers as well as the unassigned number resources.

29. *Harm to Consumers*. Rising Eagle apparently intended to harm consumers because it made spoofed robocalls that violated the TCPA. In *Roesel*, the Commission stated that "when spoofing is done in conjunction with an illegal robocalling campaign (itself a harmful practice), it indicates an intent to cause harm."[90] The Commission reasoned that harm is a broad concept that includes violations of civil statutes such as the TCPA.[91] Specifically, "the placement of illegal robocalls causes consumers significant harm, including that such calls are a nuisance and [an] invasion of privacy."[92] Spoofing exacerbates the harm from TCPA violations. It makes it impossible for consumers to accurately screen illegal calls and may coax National Do Not Call Registry listed consumers, who are otherwise wary of robocalls, to answer the phone.

30. The TCPA prohibits transmitting prerecorded or artificial voice messages to wireless phone numbers unless the called party has given consent, or the call is for an emergency purpose.[93] The TCPA also prohibits telemarketing calls without consent to residential numbers listed on the National Do Not Call Registry.[94] Evidence indicates that Rising Eagle lacked the requisite consent for its calls. Rising Eagle made at least 86,864,456 calls to wireless numbers and 56,635,935 calls to numbers on the National Do Not Call Registry, using a prerecorded voice message.[95] Bureau staff contacted multiple recipients of the robocalls at issue to confirm that they had not given permission to Rising Eagle or Health Advisors permission to call. Of the 52 people with whom Bureau staff spoke, none recalled giving Rising Eagle or Health Advisors permission to call them on their wireless phones, and 41 affirmatively stated that they did not.[96] Thus, the only probative evidence indicates that Rising Eagle lacked consent, and the calls did not fall within any other exception to the TCPA.

31. The TCPA also requires prerecorded or artificial voice message calls to state the identity of the caller at the beginning of the message as well as to include a phone number at which the caller can be reached.[97] Rising Eagle did not include this information in the prerecorded voice message calls that

---

[89] *Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6411, para. 23.

[90] *See Roesel Forfeiture Order*, 33 FCC Rcd at 9218-19, para. 40; *Abramovich Forfeiture Order*, 33 FCC Rcd at 4671, para. 27; *Abramovich Notice of Apparent Liability*, 32 FCC Rcd at 5423, para. 16.

[91] *See Roesel Forfeiture Order*, 33 FCC Rcd at 9217-18, paras. 38-39 (rejecting claim that the Truth in Caller ID Act only applies to criminal or malicious conduct).

[92] *Id.* at 9218, para. 40.

[93] 47 U.S.C. § 227(b)(1)(A)(iii); 47 CFR § 64.1200(a)(1). Calls made solely to collect a debt owed to or guaranteed by the United States are also exempted from this prohibition. 47 U.S.C. § 227(b)(1)(A)(iii).

[94] 47 U.S.C. § 227(c); 47 CFR § 64.1200(c)(2).

[95] Call Detail Records. Calls to wireless numbers and National Do Not Call Registry listed numbers may overlap as consumers may register wireless numbers that are used for residential purposes. *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 18 FCC Rcd 14014, 14039, para. 36 (2003).

[96] Declaration of {[ ]} (Apr. 8, 2020) (on file in EB-TCD-18-00027781); Declaration of {[ ]} (Apr. 6, 2020) (on file in EB-TCD-18-00027781); Declaration of {]} (Mar. 12, 2020) (on file in EB-TCD-18-00027781); Declaration of {[ ]} (Mar. 10, 2020) (on file in EB-TCD-18-00027781); Declaration of {[ ]} (Mar. 9, 2020) (on file in EB-TCD-18-00027781).

[97] 47 U.S.C. § 227(d)(3)(A); 47 CFR § 64.1200(b)(2).

Bureau staff examined. Staff obtained copies of Rising Eagle's robocall messages by reviewing voice mail recording files provided by YouMail.[98] The messages fail to provide any accurate identifying information about the caller. Rising Eagle's violation of the TCPA and the Commission's rules in conjunction with caller ID spoofing indicates an intent to harm consumers.

32. The evidence shows that Rising Eagle was familiar with the TCPA requirements and knew that it was violating them. Rising Eagle, through its RPG Leads business name, holds itself out as a provider of telemarketing services.[99] Thus Rising Eagle knew or should have known about the TCPA requirements and restrictions that govern telemarketing.[100] Further, the evidence shows that Rising Eagle intentionally violated the TCPA by calling numbers that it knew were on the National Do Not Call Registry, by disabling this feature of the calling platform it used.[101] Because it willfully violated the TCPA provisions that are intended to protect consumers, we find that Rising Eagle apparently intended to harm consumers.

33. *Harm to Carriers*. In *Abramovich*, the Commission determined that spoofing in conjunction with a large-scale illegal robocalling campaign harms the carriers that have to handle the calls.[102] Extensive illegal robocalling can overwhelm a network's capacity, and spoofing makes it harder for carriers to detect those calls and take remedial action.[103] Spoofed robocalls harm carriers by (1) burdening the carriers' networks with illegal calls, and (2) inducing enraged recipients of the illegal robocalls to complain, thereby adding to the workload of customer service agents, decreasing the perceived value of the service, and increasing carrier costs.[104] The Traceback Group and its members spent considerable resources on tracebacks to mitigate the harm caused by Rising Eagle's robocalls.[105] It was substantially certain that the millions of robocalls that Rising Eagle pumped into the national telephone network on a daily basis would burden carriers and that spoofing would delay efforts by carriers to curb the impact of the calls. Thus, we find that Rising Eagle apparently intended to harm the carriers handling its robocall traffic.

3. Rising Eagle Apparently Intended to Wrongfully Obtain Financial Compensation and Evade Liability.

34. The Truth in Caller ID Act and the Commission's rules prohibit knowingly displaying misleading or inaccurate caller ID information with the intent to wrongfully obtain anything of value.[106] We find that Rising Eagle apparently made over one billion robocalls in violation of the TCPA's identification requirements for artificial and prerecorded voice message calls and prohibition on prerecorded voice message calls to wireless numbers.[107] It also appears to have intentionally violated the

[98] YouMail Response.

[99] *See* RPG Leads, *Solutions*, https://rpgleads.com/solutions/ (last visited Feb. 6, 2020) (listing telemarketing solutions such as voice broadcasting, ringless voicemail, and predictive dialers).

[100] *See Nevada Restaurant Services, Inc. v. Clark County*, 981 F. Supp. 2d 947, 955 (D. Nev. 2013) ("Regulated businesses are responsible to make themselves aware of applicable laws and regulations.").

[101] Frankel Aff. at 2.

[102] *Abramovich Forfeiture Order*, 33 FCC Rcd at 4668, para. 17.

[103] *Id*. at 4671, para. 27.

[104] *Id*. at 4671-72, para. 27; *Abramovich Notice of Apparent Liability*, 32 FCC Rcd at 5424, para. 19.

[105] E-mail from Jessica Thompson, Manager, Policy & Advocacy, USTelecom, to Daniel Stepanicich, Attorney Advisor, FCC Enforcement Bureau (Mar. 17, 2020, 16:09 ET) (on file in EB-TCD-18-00027781).

[106] 47 U.S.C. § 227(e); 47 CFR § 64.1604.

[107] Although this NAL pertains only to apparent violations of the Truth in Caller ID Act, we take into account the fact that Rising Eagle violated the TCPA and thus acted wrongfully. With the recent passage of the TRACED Act, (continued….)

TCPA by calling consumers listed on the National Do Not Call Registry.[108] Rising Eagle apparently spoofed those unlawful calls with the intent to wrongfully obtain something of value.

35. Evidence shows that Rising Eagle was paid to make the wrongful robocalls. Rising Eagle's business model involves generating leads for call centers via illegal (i.e., wrongful) robocalls. Call centers like Health Advisors paid Rising Eagle for the leads.[109] Therefore, we find that Rising Eagle apparently knowingly spoofed numbers to wrongfully obtain something of value in the form of financial compensation.

36. Courts have held that the statutory term "anything of value" is not limited to tangible assets.[110] In this case, the spoofed robocalls apparently helped Rising Eagle evade law enforcement as well as private civil lawsuits for violations of the TCPA. The Commission has found that "avoidance of culpability is a benefit that qualifies as a thing of value."[111] Rising Eagle's attempt to evade personal TCPA liability has an ascertainable dollar value. In this case, avoidance of culpability has a specific, ascertainable dollar value—namely, up to $20,489 per unlawful call in a forfeiture action brought by the FCC.[112] Additionally, in a private action, that potential liability is up to $1,500 per illegal robocall.[113] Rising Eagle spoofed the caller ID, and omitted any identifying information that would enable consumers or investigators to reach him. In fact, many consumers mistakenly thought the calls originated from the health insurance companies that were mentioned in the robocalls or the entities to whom the spoofed numbers were assigned.[114] This obfuscation enabled Rising Eagle to avoid or defer liability for its apparently illegal robocalling campaign.

(Continued from previous page)
we may issue NALs for violations of the TCPA without first issuing a citation, and we will do so. *See* TRACED Act § 3.

[108] Bureau staff filtered Rising Eagle's Call Detail Records through an in-house do-not-call repository and found that Rising Eagle apparently placed at least 56,635,935 calls to numbers on the National Do Not Call Registry.

[109] *See* Bank of Am., Rising Eagle Global Payments Reporting U.S. Wire (Sep. 4, 2019) (Bank of Am. Wire Records) (on file in EB-TCD-18-00027781) (revealing that Health Advisors of America paid Rising Eagle Capital Group $3,219,153 between May 2018 and August 2019).

[110] *United States v. Picquet*, 963 F.2d 54, 55-56 (5th Cir. 1992) (holding that sales taxes constitute "a thing of value" for the purposes of 18 U.S.C. § 1029(a)(2)'s prohibition of using unauthorized access devices to obtain "anything of value"); *see also United States v. Singleton*, 144 F.3d 1343, 1349-50 (10th Cir. 1998), *rev'd on other grounds*, 165 F.3d 1297 (10th Cir. 1999) (agreeing with *Picquet*); *United States v. Draves*, 103 F.3d 1328, 1332 (7th Cir. 1997) (agreeing with and applying the 5th Circuit's expansive interpretation of the phrase "anything of value" in *Picquet*); *United States v. Nilsen*, 967 F.2d 539, 542-43 (11th Cir. 1992) ("Congress' frequent use of 'thing of value' in various criminal statutes has evolved the phrase into a term of art which the courts generally construe to envelope both tangibles and intangibles. This broad interpretation is based upon a recognition that monetary worth is not the sole measure of value."); *United States v. Schwartz*, 785 F.2d 673, 680 (9th Cir. 1986) (noting the broad range of intangibles that have been found to be "things of value" by prior courts); *United States v. Williams*, 705 F.2d 603, 622-23 (2nd Cir. 1983) (holding that the district court properly construed the meaning of the term "anything of value" to "focus on the value that the defendants subjectively attached to the items received"); *United States v. Sheker*, 618 F.2d 607, 609-10 (9th Cir. 1980) (holding that "value" includes anything recognized or appreciated by others); *United States v. Girard*, 601 F.2d 69, 71 (2d Cir. 1979) ("[T]he phrase ['thing of value'] is generally construed to cover intangibles as well as tangibles.").

[111] *Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6413, para. 27; *see also Roesel Forfeiture Order*, 33 FCC Rcd at 9212, para. 22.

[112] *See* 47 CFR § 1.80.

[113] 47 U.S.C. § 227(b)(3).

[114] *See supra* paras. 25-27.

C. Proposed Forfeiture

37. Section 227(e) of the Act, which empowers the FCC "to proceed expeditiously . . . without first issuing a citation[,]"[115] and section 1.80 of the Commission's rules authorize us to impose a forfeiture against any person that engages in unlawful spoofing.[116] Specifically, the Act and the Commission's rules authorize a forfeiture of up to $11,766 for each spoofing violation, or three times that amount for each day of a continuing violation, up to a statutory maximum of $1,176,638 for any single act or failure to act.[117] In exercising our forfeiture authority, we must consider the "nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[118] In addition, the Commission has established forfeiture guidelines; they establish base penalties for certain violations and identify criteria that we consider when determining the appropriate penalty in any given case.[119] Under these guidelines, we may adjust a forfeiture upward for violations that are egregious, intentional, or repeated, or that cause substantial harm or generate substantial economic gain for the violator.[120]

1. We Propose a Base Penalty of $1,000 Per Apparently Unlawful Spoofed Robocall.

38. The Commission has proposed a base forfeiture of $1,000 per unlawful spoofed robocall in past mass-spoofing enforcement actions. The Commission has applied the $1,000 amount in prior cases on the basis that the aggregate forfeiture would serve the dual goals of punishment and deterrence, and that higher amounts would be unlikely to achieve a more effective result.[121] We believe that rationale applies to this case as well and thus propose a base forfeiture amount of $1,000 per violation.

---

[115] *Truth in Caller ID Order*, 26 FCC Rcd at 9132-33, para. 47. The Truth in Caller ID Act requires that the Commission provide the notice required under section 503(b)(3) of the Act (notice and an opportunity for a hearing before the Commission or an administrative law judge) or section 503(b)(4) of the Act (Notice of Apparent Liability) before assessing a forfeiture for unlawful spoofing. 47 U.S.C. § 227(e)(5)(A). This Notice of Apparent Liability provides the required notice under section 503(b)(4) of the Act. In the TRACED Act, Congress authorized the Commission to issue a Notice of Apparent Liability, without first having to issue a warning citation, for violations of the TCPA. *Implementing Section 3 of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act*, Order, DA 20-460, paras. 6-10 (EB 2020).

[116] 47 U.S.C. § 227(e)(5); 47 CFR § 1.80(b)(4). The Truth in Caller ID Act and the Commission's rules contain a two-year statute of limitations on proposing forfeitures for unlawful spoofing. 47 U.S.C. § 227(e)(5)(A)(iv); 47 CFR § 1.80(c)(3). Unlike forfeitures assessed under section 503(b) of the Act, "the Truth in Caller ID Act does not require 'willful' or 'repeated' violations to justify imposition of a penalty." *Truth in Caller ID Order*, 26 FCC Rcd at 9133, para. 48. Thus, the Commission is not required to demonstrate the "conscious and deliberate commission or omission of such act" or that such act happened more than once or for more than one day to propose a forfeiture for apparently unlawful spoofing. 47 U.S.C. § 312(f)(1)-(2). We nevertheless find that Rising Eagle apparently willfully and repeatedly spoofed caller ID information with the intent to harm and to wrongfully obtain something of value.

[117] 47 U.S.C. § 227(e)(5)(A); 47 CFR § 1.80(b)(4). In the alternative and in lieu of the Act's general criminal penalty provisions in section 501 of the Act, the Truth in Caller ID Act also provides for criminal fines up to $10,000 for each violation, or three times that amount for each day of a continuing violation. 47 U.S.C. § 227(e)(5)(B).

[118] 47 U.S.C. § 503(b)(2)(E). The Commission stated that it would employ the statutory factors set forth in section 503(b)(2)(E) to determine the amount of a forfeiture penalty for violation of section 227(e). *Truth in Caller ID Order*, 26 FCC Rcd at 9132, para. 46.

[119] 47 CFR § 1.80(b)(8), Note to paragraph (b)(8).

[120] *Id*.

[121] Section 1.80 of the Commission's rules sets forth base forfeiture amounts for a wide variety of apparent violations. The base forfeitures in section 1.80 range from $1,000 (failure to provide station identification, for

(continued….)

39. As with past Commission actions addressing violations of section 227(e), we do not apply the base forfeiture to all 1,047,677,198 apparently unlawful spoofed calls; rather, we apply the base forfeiture to a subset of the apparently unlawful spoofed calls that has been analyzed by Bureau staff. The reasons for doing so, rather than proposing a forfeiture based on the total number of apparently spoofed calls, are pragmatic. *First*, in some cases, depending on the specific spoofing scheme, it can be time-consuming to analyze every apparently spoofed call. *Second*, in large spoofing schemes, we have found that applying a fraction of the statutory maximum per-call penalty to a fraction of the total calls results in a proposed forfeiture that achieves the dual goals of penalizing wrongful conduct and preventing it from recurring.[122] Each case is unique, and we must use our discretion in proposing an appropriate penalty to meet the specific circumstances.[123] In this case, Bureau staff analyzed 150,000 apparently unlawful spoofed calls.[124] Applying the base forfeiture to these analyzed violations yields a total base forfeiture of $150,000,000.

2. Rising Eagle's Egregious Actions Warrant a Significant Upward Adjustment to the Base Penalty.

40. In addition to the base forfeiture above, we apply the statutory factors in section 503 of the Act and section 1.80 of the Commission's rules[125] to the conduct at issue to determine an appropriate forfeiture amount. Accordingly, we consider the harm that Rising Eagle caused, the scale and scope of the unlawful spoofing campaign, and Rising Eagle's culpability for the apparent violations—and we find that the circumstances in this case warrant a significant upward adjustment to the base penalty.

41. Rising Eagle's robocall campaign is the largest in magnitude that the Commission has ever encountered—more than one billion robocalls. These robocalls were egregious because they were apparently connected with a fraudulent telemarketing scheme. Rising Eagle's calls misled consumers into thinking that the robocalls originated from well-known and reputable health insurance companies. As a result, these companies were inundated with complaints from angry consumers as well as TCPA lawsuits. Rising Eagle also apparently used each spoofed number to make millions of calls, overwhelming innocent third parties with angry call-backs from aggrieved consumers. At least one third party, Genworth, had its telephone network overwhelmed with so many call-backs from aggrieved consumers called by Rising Eagle that some Genworth employees were unable to use its phone system.[126] Additionally, Rising Eagle is highly culpable. Mr. Spiller told the Traceback Group and its representative that he knew that he was using spoofed numbers. He also allegedly admitted that he intended to make prohibited telemarketing robocalls to numbers on the National Do Not Call Registry because he received a material benefit by breaking the law—*more people answered his calls*.[127] Rising Eagle continued to make abusive robocalls despite being warned by the Traceback Group on multiple occasions that the calls were unlawful and generating complaints.[128] We find that Rising Eagle is highly culpable and its behavior is egregious. We

(Continued from previous page)
example) to the statutory maximum (misrepresentation/lack of candor). In *Abramovich,* we found that establishing the base forfeiture amount of $1,000 was reasonable. *Abramovich NAL*, 32 FCC Rcd at 5426, para. 25, n.56.

[122] *Affordable Notice of Apparent Liability*, 33 FCC Rcd at 9245-46, paras. 34-35; *Roesel Forfeiture Order*, 33 FCC Rcd at 9225, paras. 57-58; *Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6414, paras. 32-33.

[123] *See RKO General, Inc. v. FCC*, 670 F.2d 215, 237 (D.C. Cir. 1981), *cert. denied*, 456 U.S. 927 (1982) (citing *Leflore Broadcasting Co. v. FCC*, 636 F.2d 454, 463 (D.C. Cir. 1980) ("We have made it clear in earlier cases that 'the choice of remedies and sanctions is a matter wherein the Commission has broad discretion.'")).

[124] Reviewed Call Detail Records (on file in EB-TCD-18-00028267) (containing the call records Bureau staff selected for analysis, including the date and times the calls were made).

[125] 47 U.S.C. § 503(b)(2)(E); 47 CFR § 1.80; *Truth in Caller ID Order*, 26 FCC Rcd at 9132, para. 46.

[126] Genworth Aff. at 1.

[127] Frankel Aff. at 2.

[128] *Id.*

therefore propose a 50% upward adjustment to the base penalty yielding a total forfeiture amount of $225,000,000.[129]

3. We Propose to Pierce the Corporate Veil of Rising Eagle Capital Group LLC and Hold John Spiller and Jakob Mears Personally Liable as the Company's Sole Directors and Officers.

42. We find that Mr. Spiller and Mr. Mears may be held personally liable for Rising Eagle Capital Group's actions under the principle of piercing the corporate veil.[130] The Commission may pierce the corporate veil to "prevent reliance on [the] corporate form to frustrate our efforts to implement core statutory provisions."[131] To pierce the corporate veil under federal common law, it must be shown that (1) there is a unity of interest and ownership such that "the personalities and assets of the corporation and the individuals are indistinct[,]" and (2) "adherence to the corporate form would sanction a fraud, promote injustice, or lead to an evasion of legal obligations."[132]

43. A unity of interest may exist where a company's directors have commingled corporate and individual funds, assets, or affairs.[133] Mr. Spiller apparently used Rising Eagle's corporate bank account to make numerous personal expenditures.[134] Mr. Spiller further commingled funds by using a single PayPal account to facilitate hundreds of personal and corporate transactions.[135] From this account, Mr. Spiller made rent payments for his personal residence and purchased thousands of dollars' worth of goods and services that do not appear to have any relationship to Rising Eagle's business operations.[136] Similarly, Mr. Mears used corporate funds for thousands of dollars' worth of gifts for family members.[137]

---

[129] *Abramovich Forfeiture Order*, 33 FCC Rcd at 4671, para. 25.

[130] *Spring Street Partners-IV, L.P. v. Lam*, 730 F.3d 427, 443 (2013) ("Veil-piercing and 'alter ego' principles apply equally to corporations and LLCs [under Texas law].").

[131] *Telseven, LCC, Patrick Hines*, Forfeiture Order, 31 FCC Rcd 1629, 1635 (2016); *see also United States Through Small Business Admin. v. Pena*, 731 F.2d 8, 12 (D.C. Cir. 1984) ("Where the statutory purpose could be easily frustrated through the use of separate corporate entities a regulatory commission is entitled to look through corporate entities and treat the separate entities as one for purposes of regulation.") (quoting *Capital Tel. Co., Inc. v. FCC*, 498 F.2d 734, 738 & n.10 (D.C. Cir. 1974)); *General Tel. Co. of Southwest v. United States*, 449 F.2d 846, 855 (5th Cir. 1971).

[132] *N.L.R.B. v. West Dixie Enterprises, Inc.*, 190 F.3d 1191, 1194 (11th Cir. 1999) (quoting *White Oak Coal Co.*, 318 N.L.R.B. 732, 735 (1995), *enforced*, 81 F.3d 150 (4th Cir. 1996)). Federal common law rather than state law applies when a federal statutory scheme is at issue. *See id.* (applying federal common law in a case arising in Florida involving violations of federal labor statutes).

[133] *West Dixie Enterprises, Inc.*, 190 F.3d at 1194.

[134] Based on our examination of relevant banking records, such expenditures include tens of thousands of dollars in civil settlements and criminal defense fees for litigation unrelated to the operations of Rising Eagle, tens of thousands of dollars' worth of gifts paid to Mr. Spiller's girlfriend, and many thousands of dollars in gifts for Mr. Spiller's and Mr. Mears' family members and friends. *See* Bank of Am. Wire Records; *see also* Cashier's Check No. 1646710735 from Rising Eagle Capital Group to Margarita Casanova (June 15, 2019) (on file in EB-TCD-18-00027781).

[135] *See* PayPal, Global Investigations Report for Dates May 1, 2018 – Dec. 30, 2018 (Sep. 29, 2019) (2018 PayPal Transactions) (on file in EB-TCD-18-00027781); PayPal, Global Investigations Report for Dates Jan. 1, 2019 – Sept. 17, 2019 (Sep. 29, 2019) (2019 PayPal Transactions) (on file in EB-TCD-18-00027781).

[136] Mr. Spiller's personal expenditures apparently included watches, jewelry, furniture, guided meditations, comic books, online dating subscriptions, and automobile accessories. Mr. Spiller also used commingled funds to purchase tens of thousands of dollars of in-game currency for various smartphone games. *See* 2018 PayPal Transactions; 2019 PayPal Transactions.

[137] Bank of Am. Wire Records; 2018 PayPal Transactions; 2019 PayPal Transactions.

Finally, Mr. Spiller allowed non-officers access to the commingled PayPal account to make corporate payments as well as personal purchases for themselves totaling hundreds of dollars.[138]

44. Mr. Spiller's and Mr. Mears' unity of interest and ownership is further evinced by the fact that they alone directed Rising Eagle's apparently unlawful robocalling scheme. The Commission has found that "personal liability is appropriate (and the Commission will pierce the corporate veil) where the individual . . . is an officer of a closely held corporation and directly participates in, oversees, authorizes or otherwise directs the commission of the wrongful act."[139] Here, Mr. Spiller and Rising Eagle share the same Houston address, which, according to Texas property records, is a single-family residence owned by Mr. Spiller's girlfriend.[140] At all times relevant to this Notice of Apparent Liability, Mr. Spiller served as founder, managing member, and director of Rising Eagle, while Mr. Mears served as director, managing member, and agent for service of legal process on the company.[141] Mr. Spiller and Mr. Mears served as the Company's only two directors and officers.[142] In these capacities, Mr. Spiller and Mr. Mears acted for and were employed by Rising Eagle.[143] Mr. Spiller spoke on behalf of Rising Eagle, possessed intimate knowledge of the details of the apparently unlawful robocalling campaign, and both Mr. Spiller and Mr. Mears acted as points of contact for inquiries into Rising Eagle's business practices.[144] Those practices included using telemarketing to sell health insurance by means of apparently unlawfully spoofed robocalls. To that end, the evidence shows that Mr. Spiller and Mr. Mears made or caused to be made 1,047,677,198 spoofed robocalls in a mere four-and-a-half-month period.[145]

---

[138] *Supra* note 135 (indicating that a non-officer used the PayPal account to purchase and ship camouflage equipment, jewelry, and automobile parts to his or her personal address).

[139] *Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6416, para. 34.

[140] *Compare* Real Property Records, Account No. 1263930010025, Harris Cty. Appraisal Dist. (providing ownership and property information for 9022 N Ferndale Place Dr., Houston, TX 77064), *with* Rising Eagle Capital Group LLC, Statement of Change of Registered Office/Agent, Office of the Sec'y of State of Tex. (June 10, 2019) (showing that the personal address of Mr. Spiller's girlfriend is also the business address of Rising Eagle Capital Group LLC).

[141] *See* Rising Eagle Capital Group LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Apr. 9, 2014); Rising Eagle Capital Group LLC, Certificate of Amendment, Office of the Sec'y of State of Tex. (June 1, 2018) (adding Jakob Mears as a member and director); Rising Eagle Capital Group LLC, Public Information Report, Office of the Sec'y of State of Tex. (2018); *see also* Rising Eagle Capital Group LLC, Taxable Entity Search, Tex. Comptroller of Pub. Accounts (information collected Dec. 11, 2019), https://mycpa.cpa.state.tx.us/coa/search.do (search Entity Name field for "Rising Eagle Capital Group LLC" and select the "Search" button; then select "Details") (showing Jakob Mears as the Registered Agent of Rising Eagle Capital Group LLC).

[142] *See supra* note 141.

[143] *See id.*; *see also* 2018 PayPal Transactions; 2019 PayPal Transactions; Bank of Am. Wire Records; Frankel Aff. at 2–5.

[144] Frankel Aff. at 4-5; USTelecom Subpoena Response (Oct. 23, 2019) (on file in EB-TCD-18-00027781).

[145] Pursuant to section 217 of the Act, when "enforcing the provisions of this chapter, the act, omission, or failure of any officer . . . acting for or employed by any . . . user, acting within the scope of his employment, shall in every case be also deemed to be the act, omission, or failure of such . . . user as well as that of the person." 47 U.S.C. § 217. Rising Eagle Capital Group LLC, Rising Eagle Capital Group – Cayman, Only Web Leads, LLC, and JSquared Telecom, LLC are "users" of the telephone networks to engage in illegal robocalling. *See Scott Malcolm DSM Supply, LLC Somaticare, LLC*, Notice of Apparent Liability, 29 FCC 2476, 2484, para. 19 (2014) (determining that a TCPA violator is a user as contemplated by section 217). Thus, the acts and omissions of Mr. Spiller and Mr. Mears may be imputed to Rising Eagle Capital Group LLC as well as to the individual directors.

45. Treating Rising Eagle, Mr. Spiller, and Mr. Mears as separate entities would sanction an apparent fraud, promote injustice, or lead to an evasion of legal obligations.[146] Rising Eagle apparently has engaged in a fraudulent scheme to misrepresent well-known insurance companies and mislead consumers into purchasing its clients' products directed by Messrs. Spiller and Mears as the only members and directors of the company.[147] Mr. Spiller and Mr. Mears diverted Rising Eagle's corporate assets to fund substantial personal expenses, including personal rent payments and legal settlements,[148] which enriched themselves while limiting Rising Eagle's ability to satisfy remedial obligations.[149] Additionally, failure to pierce the corporate veil would promote injustice by frustrating the Commission's ability to perform its statutory mandate of preventing unlawful robocalls. Mr. Spiller and/or Mr. Mears have collectively formed no fewer than a dozen companies and at least 26 business names in multiple states and territories, many of which are lead generation or insurance sales entities.[150] For these reasons, adherence to the corporate form would allow Mr. Spiller and Mr. Mears to easily shut down and open new companies like Rising Eagle with impunity.[151]

4. We Propose to Hold John Spiller, Jakob Mears, Rising Eagle Capital Group LLC, JSquared Telecom LLC, Rising Phoenix Group, Rising Phoenix

[146] *See S.E.C. v. Hickey*, 322 F.3d 1123, 1128 (9th Cir. 2003) (discussing the test for piercing the corporate veil in California); *Ministry of Defense of the Islamic Republic of Iran v. Gould, Inc.*, 969 F.2d 764, 769 n.3 (9th Cir. 1992) (observing that federal and California law are substantially similar on the issue of piercing the corporate veil); *see also Estate of Salm v. N.L.R.B.*, 509 F. App'x 94, 95 (2nd Cir. 2013) (citing *White Oak Coal Co.*, 318 N.L.R.B 732, 734-35 (1995)).

[147] Blue Cross Aff. at 1-2; Cigna Aff. at 1-2.

[148] *See* 2018 PayPal Transactions; 2019 PayPal Transactions; Bank of Am. Wire Records.

[149] *N.L.R.B. v. West Dixie Enterprises, Inc.*, 190 F.3d 1191, 1194 (11th Cir. 1999) ("With regard to the second prong of the test, whether a finding of no personal liability 'would sanction a fraud, promote injustice, or lead to an evasion of legal obligations,' . . . [Company] funds were used to pay rent on [the director's] personal apartment for six months, and the [directors] have failed to produce records showing that this arrangement constituted anything but a diversion of corporate assets for personal use.").

[150] *See* Ciw Group LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (May 7, 2013) (terminated Mar. 12, 2014); Developing Group, Certificate of Formation, Office of the Sec'y of State of Tex. (Jan. 15, 2014) (terminated Jan. 26, 2018); Rising Eagle Capital Group LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Apr. 9, 2014) (also conducted business as Archimedes Funding, JP's Web Leads, Only Web Leads, Rising Phoenix Holdings, RPG Leads, Senior Med Alert LLC, and Travel Destination Adventures Your Wish Is Our Desire) (terminated Feb. 28, 2020); Lightning Strikes Lead Generation LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Oct. 27, 2015) (terminated Jan. 27, 2017); L&J Lead Generation LLC, Electronic Articles of Organization, Fla. Dep't of State, Division of Corporations (Mar. 22, 2016); Anmac Roofing LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Mar. 30, 2018) (also doing business as Anmac Construction); Right Start Health & Life Insurance LLC, Electronic Articles of Organization, Fla. Dep't of State, Division of Corporations (Apr. 17, 2018); Only Web Leads LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Nov. 20, 2018); JSquared Telecom LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Jan. 30, 2019) (also doing business as Connect Express, Express Connect, and Jump Start Business Ventures); Jakobs M Group, Certificate of Formation, Office of the Sec'y of State of Tex. (June 4, 2019); MJ Capital Investment LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Oct. 12, 2019); Rising Eagle Capital Group – Cayman, Search Report, Cayman Is. General Registry (Oct. 16, 2019); Mental Health Care Solutions LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Jan. 9, 2020) (also doing business as Elderly Care Solutions and Give a Heart for the Homeless).

[151] *See Abramovich Notice of Apparent Liability*, 32 FCC Rcd at 5428, para. 27; Rising Eagle Capital Group LLC, Certificate of Amendment, Office of the Sec'y of State of Tex. (Jan. 13, 2020) (replacing Mr. Spiller and Mr. Mears as directors with Rising Eagle Capital Group Cayman Artemis House and terminating Rising Eagle Capital Group LLC shortly thereafter). *See generally supra* note 150 (evincing a pattern of frequent formation and termination of business entities).

Holdings, RPG Leads, and Any Successors in Interest Jointly and Severally Liable.

46. Just as Mr. Spiller and Mr. Mears acted as the sole directors of Rising Eagle, Rising Eagle was the sole manager of both Only Web Leads LLC and JSquared Telecom LLC.[152] Mr. Spiller's and Mr. Mears' fiduciary duties as sole directors—and control as sole board members—of Rising Eagle dictate that Rising Eagle, Only Web Leads, and JSquared Telecom knew and approved of Mr. Spiller's and Mr. Mears' apparently unlawful use of the telephone network to transmit spoofed robocalls with the apparent intent to cause harm, defraud, or obtain anything of value.[153]

47. Besides Rising Eagle, Only Web Leads, and JSquared Telecom, Mr. Spillers and Mr. Mears also did business as Rising Phoenix Group,[154] Rising Phoenix Holdings,[155] and RPG Leads;[156] however, these are not formal legal entities as they possess no corporate, partnership, or other business entity filings. We treat Rising Phoenix Group, Rising Phoenix Holdings, and RPG Leads as mere unincorporated associations of Mr. Spiller and Mr. Mears and hold each jointly and severally liable along with Mr. Spiller and Mr. Mears, to the extent they have any independent legal existence, for the violations found herein. For the foregoing reasons, we hold both Mr. Spiller and Mr. Mears jointly and severally liable with Rising Eagle Capital Group LLC, Only Web Leads, LLC, JSquared Telecom, LLC, Rising Phoenix Group, Rising Phoenix Holdings, and RPG Leads for the proposed forfeiture.

48. Lastly, Mr. Spiller formed Rising Eagle Capital Group – Cayman, an offshore company located in the Cayman Islands, on October 16, 2019.[157] On January 13, 2020, Mr. Spiller and Mr. Mears filed a Certificate of Amendment for Rising Eagle Capital Group LLC with the Texas Secretary of State, removing themselves as managing members and adding Rising Eagle Capital Group Cayman Artemis House as the new, sole managing member.[158] Mr. Spiller and Mr. Mears dissolved Rising Eagle Capital Group LLC on February 28, 2020.[159] Mr. Spiller then ceased using the name "Rising Eagle Capital Group" in communications with a Traceback Group consultant, instead choosing to correspond under the

---

[152] JSquared Telecom LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Jan. 30, 2019); Only Web Leads LLC, Certificate of Formation, Office of the Sec'y of State of Tex. (Nov. 20, 2018).

[153] Mr. Spiller used Rising Eagle's corporate bank accounts to make telemarketing related payments. *See* 2018 PayPal Transactions; 2019 PayPal Transactions; Bank of Am. Wire Records; *see also AngioScore, Inc. v. TriReme Medical, Inc.*, 87 F.Supp.3d 986, 1002-03 (N.D. Cal. Apr. 6, 2015) (outlining the breath of the fiduciary duty owed a corporation and corporate opportunity doctrine).

[154] Mr. Spiller used the business name "Rising Phoenix Group" apparently synonymously with "Rising Eagle Capital Group" in a large number of business-related transactions conducted through Rising Eagle Capital Group's corporate bank account. *See* Bank of Am. Wire Records.

[155] Rising Eagle Capital Group LLC, Assumed Name Certificate, Office of the Sec'y of State of Tex. (Jan. 12, 2015) (creating the assumed name of Rising Phoenix Holdings).

[156] Rising Eagle Capital Group LLC, Assumed Name Certificate, Office of the Sec'y of State of Tex. (Mar. 17, 2017) (creating the assumed name of RPG Leads).

[157] Rising Eagle Capital Group – Cayman, Search Report, Cayman Is. General Registry (Oct. 16, 2019) (providing a Registration Number of 356487 and registered office at WB Corporate Services (Cayman) Ltd., P.O. Box 2775, 1st Floor Artemis House, 67 Fort Street, George Town, Grand Cayman KY1-1111, Cayman Islands).

[158] Rising Eagle Capital Group LLC, Certificate of Amendment, Office of the Sec'y of State of Tex. (Jan. 13, 2020). Rising Eagle Capital Group – Cayman and Rising Eagle Capital Group Cayman Artemis House appear to be the same entity, as both entities list the same Cayman Islands address and the Cayman Islands General Registry does not have a record of registration for any entity named Rising Eagle Capital Group Cayman Artemis House. *See id.*; Rising Eagle Capital Group – Cayman, Search Report, Cayman Is. General Registry (Oct. 16, 2019).

[159] Rising Eagle's termination occurred well-after the apparently unlawful activities that form the basis of this Notice of Apparent Liability. Rising Eagle Capital Group LLC, Forfeiture of Certification, Office of the Sec'y of State of Tex. (Feb. 28, 2020).

name "Rising Eagle Capital Group Cayman."[160] As the successor in interest to Rising Eagle Capital Group LLC and to discourage asset-shifting in anticipation of a forfeiture, we hold Rising Eagle Capital Group – Cayman jointly and severally liable with the above-named entities.[161]

IV. ORDERING CLAUSES

49. Accordingly, **IT IS ORDERED** that, pursuant to section 503(b) of the Act[162] and section 1.80 of the Commission's rules,[163] John C. Spiller, Jakob A. Mears, Rising Eagle Capital Group LLC, JSquared Telecom LLC, Only Web Leads LLC, Rising Phoenix Group, Rising Phoenix Holdings, RPG Leads, and Rising Eagle Capital Group – Cayman are hereby **NOTIFIED** of this **APPARENT LIABILITY FOR A FORFEITURE** in the amount of two hundred, twenty-five million dollars ($225,000,000) for willful and repeated violations of section 227(e) of the Act;[164] section 64.1604 of the Commission's rules;[165] and the *Rules and Regulations Implementing the Truth In Caller ID Act of 2009* and associated rules.[166]

50. **IT IS FURTHER ORDERED** that, pursuant to section 1.80 of the Commission's rules,[167] within thirty (30) calendar days of the release date of this Notice of Apparent Liability for Forfeiture, John C. Spiller, Jakob A. Mears, Rising Eagle Capital Group LLC, JSquared Telecom LLC, Only Web Leads LLC, Rising Phoenix Group, Rising Phoenix Holdings, RPG Leads, and Rising Eagle Capital Group – Cayman **SHALL PAY** the full amount of the proposed forfeiture or **SHALL FILE** a written statement seeking reduction or cancellation of the proposed forfeiture, consistent with paragraphs 53-54 below.

51. John C. Spiller, Jakob A. Mears, Rising Eagle Capital Group LLC, JSquared Telecom LLC, Only Web Leads LLC, Rising Phoenix Group, Rising Phoenix Holdings, RPG Leads, and Rising Eagle Capital Group – Cayman shall send electronic notification of payment to Lisa Williford at Lisa.Williford@fcc.gov on the date said payment is made. Payment of the forfeiture must be made by credit card, ACH (Automated Clearing House) debit from a bank account using the Commission's Fee Filer (the Commission's online payment system),[168] or by wire transfer. The Commission no longer accepts forfeiture payments by check or money order. Below are instructions that payors should follow based on the form of payment selected:[169]

---

[160] Frankel Aff. at 4-5.

[161] A successor corporation is liable for its predecessor's liabilities and debts if the creation of the successor entity constitutes a de facto merger or consolidation with the prior entity, the successor is a mere continuation of the prior entity, and/or the successor exists in order to fraudulently escape liability for such debts. *See Ronnoco Coffee, LLC v. Westfeldt Brothers, Inc.*, 939 F.3d 914, 920-21 (8th Cir. 2019); *Corrigan v. U.S. Steel Corp.*, 478 F.3d 718, 726-27 (6th Cir. 2007); *Reese Bros. Inc. v. U.S. Postal Service*, 477 F.Supp.2d 31, 40-41 (D.D.C. 2007). In the present case, Rising Eagle Capital Group – Cayman became the sole director of Rising Eagle Capital Group prior to the latter's dissolution shortly thereafter, and Mr. Spiller and Mr. Mears have continued to place robocalls since Rising Eagle Capital Group's dissolution. Rising Eagle Capital Group LLC, Certificate of Amendment, Office of the Sec'y of State of Tex. (Jan. 13, 2020).

[162] 47 U.S.C. § 503(b).

[163] 47 CFR § 1.80.

[164] 47 U.S.C. § 227(e).

[165] 47 CFR § 64.1604.

[166] *Truth in Caller ID Order*.

[167] 47 CFR § 1.80.

[168] Payments made using the Commission's Fee Filer system do not require the submission of an FCC Form 159.

[169] For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #6), or by e-mail at ARINQUIRIES@fcc.gov.

- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. A completed Form 159 must be faxed to the Federal Communications Commission at 202-418-2843 or e-mailed to RROGWireFaxes@fcc.gov on the same business day the wire transfer is initiated. Failure to provide all required information in Form 159 may result in payment not being recognized as having been received. When completing FCC Form 159, enter the Account Number in block number 23A (call sign/other ID), enter the letters "FORF" in block number 24A (payment type code), and enter in block number 11 the FRN(s) captioned above (Payor FRN).[170] For additional detail and wire transfer instructions, go to https://www.fcc.gov/licensing-databases/fees/wire-transfer.
- Payment by credit card must be made by using the Commission's Fee Filer website at https://apps.fcc.gov/FeeFiler/login.cfm. To pay by credit card, log-in using the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Pay bills" on the Fee Filer Menu, and select the bill number associated with the NAL Account – the bill number is the NAL Account number with the first two digits excluded – and then choose the "Pay by Credit Card" option. Please note that there is a $24,999.99 limit on credit card transactions.
- Payment by ACH must be made by using the Commission's Fee Filer website at https://apps.fcc.gov/FeeFiler/login.cfm. To pay by ACH, log in using the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Pay bills" on the Fee Filer Menu and then select the bill number associated to the NAL Account – the bill number is the NAL Account number with the first two digits excluded – and choose the "Pay from Bank Account" option. Please contact the appropriate financial institution to confirm the correct Routing Number and the correct account number from which payment will be made and verify with that financial institution that the designated account has authorization to accept ACH transactions.

52. Any request for making full payment over time under an installment plan should be sent to: Chief Financial Officer—Financial Operations, Federal Communications Commission, 445 12th Street, SW, Room 1-A625, Washington, DC 20554.[171] Questions regarding payment procedures should be directed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES@fcc.gov.

53. The written statement seeking reduction or cancellation of the proposed forfeiture, if any, must include a detailed factual statement supported by appropriate documentation and affidavits pursuant to sections 1.16 and 1.80(f)(3) of the Commission's rules.[172] The written statement must be mailed to the Office of the Secretary, Federal Communications Commission, 445 12th Street, SW, Washington, DC 20554, ATTN: Enforcement Bureau – Telecommunications Consumers Division, and must include the NAL/Account Number referenced in the caption. The statement must also be e-mailed to Shana Yates, Assistant Division Chief, Telecommunications Consumers Division, at Shana.Yates@fcc.gov, and Daniel Stepanicich, Attorney, Telecommunications Consumers Division, at daniel.stepanicich@fcc.gov.

[170] Instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

[171] *See* 47 CFR § 1.1914.

[172] *Id*. at §§ 1.16, 1.80(f)(3).

54. The Commission will not consider reducing or canceling a proposed forfeiture in response to a claim of inability to pay unless the petitioner submits the following documentation: (1) federal tax returns for the past three years; (2) financial statements for the past three years prepared according to generally accepted accounting practices; or (3) some other reliable and objective documentation that accurately reflects the petitioner's current financial status.[173] Any claim of inability to pay must specifically identify the basis for the claim by reference to the financial documentation. Inability to pay, however, is only one of several factors that the Commission will consider in determining the appropriate forfeiture, and we have discretion to not reduce or cancel the forfeiture if other prongs of 47 U.S.C. § 503(b)(2)(E) support that result.[174]

55. **IT IS FURTHER ORDERED** that a copy of this Notice of Apparent Liability for Forfeiture together with the Reviewed Call Detail Records shall be sent by first class mail and certified mail, return receipt requested, to John C. Spiller, Rising Eagle Capital Group LLC, JSquared Telecom LLC, Rising Eagle Phoenix Group, Rising Phoenix Holdings, and RPG Leads at {[ ]}, Jakob A. Mears at {[ ]}, Rising Eagle Capital Group – Cayman at WB Corporate Services (Cayman) Ltd., P.O. Box 2775, 1st Fl. Artemis House, 67 Fort Street, George Town, Grand Cayman KYI-1111, Cayman Islands, and Only Web Leads LLC at 10807 Wickersham Ln., Houston, TX 77042.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[173] 47 U.S.C. § 503(b)(2)(E).

[174] *Abramovich Forfeiture Order*, 33 FCC Rcd at 4678-79, paras. 44-45.

STATEMENT OF
CHAIRMAN AJIT PAI

Re: *John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, File No.: EB-TCD-18-00027781.

The COVID-19 pandemic has disrupted businesses across the nation, displaced the American workforce, shuttered sports leagues, and closed our children's schools. But there is one thing the pandemic hasn't dampened—our commitment to protect the American people from illegal robocallers. Indeed, in a first-of-its-kind effort in April, we partnered with the Federal Trade Commission to send cease and desist letters to three gateway providers that were facilitating the delivery of COVID-19-related scam robocalls into the United States. We told them that if they didn't stop bringing these unlawful robocalls into the country, they would be at risk of entirely losing access to our nation's phone system. Within 24 hours of our sending these letters, those providers stopped carrying those scam robocalls. Then, in May, we did it again with the U.S. Department of Justice now on board. And again, three different gateway providers stopped bringing COVID-19-related scam robocalls into the United States within 24 hours of receiving the letters.

Today's Notice of Apparent Liability is the latest action taken by the Commission to combat illegal robocalls since the COVID-19 pandemic was declared a national emergency. It proposes a landmark forfeiture of $225,000,000—the largest fine ever in FCC history. That's because operating through various companies—collectively, Rising Eagle—John C. Spiller and Jakob A. Mears made approximately one billion spoofed robocalls—yes, that's billion with a "b"—in the first four-and-a-half months of 2019 with the intent to defraud, cause harm, and wrongfully obtain something of value, in apparent violation of the Truth in Caller ID Act.

Like other nefarious robocalling scams, Rising Eagle primarily used spoofed Caller ID numbers to flood consumers with prerecorded calls. The robocalls misled consumers into thinking that the calls were from well-known and reputable health insurance providers, such as Cigna and Blue Cross Blue Shield. But that was far from the truth. Instead, the unsuspecting recipients of these robocalls were transferred to Rising Eagle's clients, which attempted to sell them short-term, limited-duration health insurance plans offered by lesser known entities—a far cry from expectations.

One disabled and elderly recipient attested to having fallen down attempting to answer these repeated calls. The scam also caused the companies whose Caller IDs were spoofed by Rising Eagle to become overwhelmed with angry call-backs from aggrieved consumers. At least one company was hit with several lawsuits because its number was spoofed, and another was so overwhelmed with calls that its telephone network became unusable.

What made Mr. Spiller's scheme so insidious from a consumer perspective was something he admitted to investigators. Not only did he make millions of calls a day using spoofed numbers, but he took particular care to include customers who had put their names on the National Do Not Call Registry—because he "found his sales rates . . . rose substantially" when he did so. Rising Eagle even continued to make abusive robocalls despite being warned on multiple occasions that the calls were unlawful and were generating complaints.

Thankfully, Rising Eagle's scam has now run its course. And I think it's important to highlight that this enforcement action was made possible, in part, thanks to a collaborative and ongoing effort between our own Enforcement Bureau staff and experts from the USTelecom Industry Traceback Group. Along with our action to clamp down on COVID-19-related robocall scams with the Federal Trade Commission and the Department of Justice, today's NAL is another example of how collaboration across government and with industry can bring robocallers to justice.

I want to thank our intrepid staff for their diligent work in bringing this action before the Commission: Lisa Gelb, Rosemary Harold, Jermaine Haynes, Shannon Lipp, Nakasha Ramsey, Sonja

Rifken, Linda Sims, Daniel Stepanicich, Kristi Thompson, Brandon Thompson, Kimberly Thorne, Bridgette Washington, Lisa Williford, and Shana Yates of the Enforcement Bureau; Eduard Bartholme, Kurt Schroeder, and Mark Stone of the Consumer Governmental Affairs Bureau; Rachel Kazan, Susan Lee, Ginny Metallo, and Emily Talaga of the Office of Economics and Analytics; Valerie Hill, Rick Mallen, and Bill Richardson of the Office of General Counsel; and Daniel Kahn and Melissa Droller Kirkel of the Wireline Competition Bureau.

STATEMENT OF
COMMISSIONER BRENDAN CARR

Re: *John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, File No.: EB-TCD-18-00027781.

Illegal robocalls are the FCC's top consumer complaint. And for good reason. They're not only annoying and disruptive, fraudsters bombard Americans with these calls to steal their money. That is why I'm glad that this FCC elevated robocalls to our top enforcement priority.

Since many of those placing these illegal calls operate overseas, we issued new rules to crack down on international robocalls and have begun working with international partners to trace them back and shut them down. We authorized carriers to block calls that they believe are part of illegal robocalling schemes, just like Gmail blocks your spam. And while industry is in the best position to develop network-based solutions, we have pushed the industry to move quickly on implementing solutions like STIR/SHAKEN, which can prevent fraudsters from spoofing phone numbers.

Our enforcement action today represents a major win for the industry-led approach. A consortium of telecom companies called the Industry Traceback Group used its members' data to identify the origin of these apparent scam calls, and it then passed that information over to our enforcement staff. The conduct at issue in this case appears particularly troublesome, as it was not merely about annoying calls interrupting dinner. The calls in this case appear designed to defraud Americans on health insurance.

So I want to thank the staff of the Enforcement Bureau, the Consumer and Governmental Affairs Bureau, and the Wireline Competition Bureau – as well as the Industry Traceback Group – for their hard work on this item. It has my support.

STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL

Re: *John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, File No.: EB-TCD-18-00027781.

We're all sick of robocalls. But if you're like me you especially despise those that come in with a number designed to look familiar—like friends and family—so you instinctively pick up the line. These spoofed calls are more than a nuisance. They're fraud.

So today it's good news that the Federal Communications Commission proposes its largest-ever fine penalizing a robocalling operation that spoofed numbers to hawk healthcare policies. These scam artists lied and said they were calling on behalf of well-known health insurance companies on more than a billion calls. That's fraud on an enormous scale. So in this Notice of Apparent Liability we propose to penalize them with a $225 million fine.

That sounds right. It's also right that in the wake of our vote today a group of state attorneys general is going to file action against these robocallers in federal court for violation of the Telephone Consumer Protection Act. In other words, this is a joint project to bring an end to an especially ugly spoofing operation. But there's something missing in this all-hands effort. That's the Department of Justice. They aren't a part of taking on this fraud. Why not? What signals does their refusal to be involved send?

Here's the signal I see. Over the last several years the FCC has levied hundreds of millions in fines against robocallers just like the folks we have here today. But so far collections on these eye-popping fines have netted next to nothing. In fact, it was last year that *The Wall Street Journal* did the math and found that we had collected no more than $6,790 on hundreds of millions in fines. Why? Well, one reason is that the FCC looks to the Department of Justice to collect on the agency's fines against robocallers. We need them to help. So when they don't get involved—as here—that's not a good sign.

Despite these problems, this notice has my support. I appreciate the work of our Enforcement Bureau to build a case against this fraud. I only wish that we had a whole-of-government effort to not only announce a big fine but do what is really meaningful—and that's collect.

STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, File No.: EB-TCD-18-00027781.

The facts are pretty clear cut here, and Messrs. Spiller and Mears appear to have merited every penny of the forfeiture we propose today for their prolific robocalling campaign. They admitted to using spoofed numbers that were not assigned to them to peddle short-term health insurance plans in over 1 billion calls. They also acknowledged intentionally making calls to consumers on the National Do Not Call Registry because they found those calls led to substantially more sales. It is particularly upsetting that these robocalls involved scams related to healthcare, given that medical communications are now more important than ever. I therefore approve this action; stopping illegal robocalls is the Commission's top consumer protection priority, and we must remain aggressive in the fight to bring consumers relief from these annoying and often harmful intrusions.

But what now? What is the plan for following through to make sure this forfeiture is paid (assuming there's something to collect) and that these offenders get out of the robocalling business for good?

According to a Wall Street Journal Article, between 2015 and March of 2019 the FCC issued forfeitures totaling $208.4 million for robocall violations, but collected only $6,790.[1] I asked the Enforcement Bureau about our progress in collecting on large forfeitures, and was told that the Bureau does not maintain a list of proposed forfeitures and collections. Notably in 2015, then Commissioner Pai observed how the Enforcement Bureau's process had "gone off the rails," in part by how "extremely hard [it is to] find out just how much money is actually being collected after the media headlines fade into the rear-view mirror."[2] He wanted the same answers then that I want now, but five years later we appear to be in the same place.

The threat of large fines as a deterrent means nothing if we systematically fail to actually collect on them, including coordinating with the Department of Justice. That means better follow-through on the entire life of an enforcement action. We must work harder to ensure on the back end that our enforcement efforts reap actual, measurable results, and then be transparent about how we're doing to put violators on notice that we mean business. Otherwise, we're just creating more headlines.

[1] Sarah Krause, The Wall Street Journal, "The FCC Has Fined Robocallers $208 Million. It's Collected $6,790." (Mar. 28, 2019) (also noting that during Ajit Pai's tenure as FCC chairman since January 2017, the FCC had issued $202 million in forfeiture orders against robocallers but had collected none of it), https://www.wsj.com/articles/the-fcc-has-fined-robocallers-208-million-its-collected-6-790-11553770803.

[2] Remarks of Commissioner Ajit Pai at the PLI/FCBA 33rd Annual Institute on Telecommunications Policy & Regulation, Washington, DC (Dec. 3, 2015), https://www fcc.gov/document/commissioner-pai-plifcba-remarks. Commissioner Pai also mentioned a then-recent POLITICO headline that read, "FCC proposes millions in fines, collects $0."