

Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of
Adrian Abramovich,
Marketing Strategy Leaders, Inc., and
Marketing Leaders, Inc.
File No.: EB-TCD-15-00020488
NAL/Acct. No.: 201732170006
FRN: 0026627141

NOTICE OF APPARENT LIABILITY FOR FORFEITURE

Adopted: June 22, 2017

Released: June 22, 2017

By the Commission: Chairman Pai and Commissioner Clyburn issuing separate statements;
Commissioner O’Rielly concurring.

I. INTRODUCTION

1. This Notice of Apparently Liability for Forfeiture (NAL) finds that Adrian Abramovich (Abramovich) is apparently liable for perpetrating one of the largest spoofed robocall campaigns that the Commission has ever investigated, involving nearly 100 million robocalls during a three-month period in 2016. Accurate caller ID information allows consumers to make informed decisions about which calls to accept, ignore, or block, and whether the party on the other end of the phone line is reputable and deserving of their trust. The Truth in Caller ID Act of 2009 and the Commission’s rules (Rules), prohibit any individual from falsifying or faking his or her phone number with the intent to defraud, cause harm, or wrongfully obtain anything of value. This prohibited practice is better known as “spoofing.” Spoofing is particularly pernicious when used to advance illegal robocalls—the number one consumer complaint received by the Federal Communications Commission (Commission or FCC). As technology has improved, the dangerous combination of spoofing and illegal robocalls has become much more potent, making illegal robocalling campaigns more deceptive, more disruptive, and harder to stop. The Enforcement Bureau (Bureau) has investigated complaints regarding Abramovich’s alleged scheme involving spoofed robocalls appearing to originate from local numbers and offering holiday vacations and cruises to popular destinations in Mexico, the Caribbean, and Florida. The callers falsely claim to be affiliated with well-known American travel and hospitality companies—including TripAdvisor, Expedia, Marriott, and Hilton—but then connect trusting consumers to unaffiliated third parties.

2. Today, the Commission issues this NAL¹ and proposes a penalty of \$120,000,000 against Mr. Adrian Abramovich² for apparently causing the display of misleading or inaccurate caller ID

¹ The Commission also released a Citation and Order notifying Abramovich that he violated the Telephone Consumer Protection Act (TCPA) and the federal wire fraud statute by making illegal robocalls to emergency lines, wireless phones, and residential phones, and that included prerecorded messages falsely claiming affiliation with well-known U.S. travel and hotel companies. Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc., Citation and Order, DA 17-593 (EB June 22, 2017) (Abramovich Citation).

² We reference Adrian Abramovich and the companies that he owns and controls as one and the same. See infra para. 27. Abramovich has formed 12 corporations in Florida over the past two decades, many of which only existed for one year before he dissolved them. He has operated the following companies: Alphavision, Inc. (Jul. 23, 1997 to Jan. 14, 2002); Telsur Communications, Inc. (June 18, 1999 to Dec. 18, 2003); Promociones Y Saldos de Remate de Mercancias Enterprise, Inc. (Sept. 12, 2002 to Sept. 19, 2003); Horizontes Promociones, Inc. (Apr. 7, 2003 to Oct. 1, 2004); Marketing Leaders, Inc. (Apr. 28, 2005 to Sept. 18, 2006); One Destinations, Inc. (July 2, 2007 to Sept. 2, 2011); One Destinations Telecom, Inc. (Jan. 5, 2009 to Sept. 23, 2011); Mundidiomas Inc. (Apr. 28, 2009 to Sept. 23, 2011); Medical Imaging Equipment, Inc. (July 20, 2012 to Sept. 27, 2013); Marketing Strategy Leaders, Inc. (Mar. 10, 2004 to Jan. 29, 2016); Emerald Media, Inc. (Sept. 21, 2015 to present); Exclusive Leads Services,

(continued....)

information with the intent to defraud, cause harm, or wrongfully obtain anything of value. The evidence shows that Abramovich apparently made 96,758,223 spoofed telephone calls over a three-month period in 2016. Abramovich apparently made the spoofed robocalls with the intent to cause consumers harm. Abramovich received payment for his work, which depended on falsely representing that the calls originated locally (to induce consumers to answer the telephone) and that the offers were affiliated with well-known hotel and travel companies (to induce consumers to pursue the offer). The spoofed numbers were an integral part of Abramovich's scheme to mislead consumers. We therefore find that Abramovich apparently violated the Truth in Caller ID Act of 2009, as codified in Section 227(e) of the Communications Act of 1934, as amended (Communications Act or Act),³ and Section 64.1604 of the Rules.⁴

II. BACKGROUND

A. The Truth in Caller ID Act of 2009

3. The Commission has long stressed the importance of requiring telemarketers to transmit accurate caller ID information. Even before the passage of the Truth in Caller ID Act, the Commission noted that "Caller ID allows consumers to screen out unwanted calls and to identify companies that they wish to ask not to call again."⁵ The Commission went on to say that "[k]nowing the identity of the caller is also helpful to consumers who feel frightened or threatened by hang-up or 'dead air' calls."⁶ The Truth in Caller ID Act of 2009 outlaws "caus[ing] any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value."⁷ Congress observed that consumers greatly value accurate, reliable caller ID information to help them decide whether to answer a phone call and, ultimately, whether to trust the caller on the other end of the line. Congress noted that consumers' widespread expectation is that any information that appears on caller ID represents the true originating number of the person or entity making the call.⁸

4. In the years leading up to the Truth in Caller ID Act's passage, consumers, telephone carriers, the Commission, and other law enforcement authorities observed a growing, troubling trend—deliberate falsification of caller ID information as part of criminal frauds and other harmful activities posing threats to the pocketbooks, privacy, and peace of mind of millions of American consumers. Congress was especially concerned by cases where criminals used spoofed caller ID information for the purposes of defrauding consumers or wrongfully obtaining something of value from the called persons. For example, Congress was aware that fraudsters could spoof the caller ID information of recognizable businesses and thus "cause people to blame innocent businesses instead of the real source for the calls."⁹ In another cited example, scammers spoofed telephone numbers belonging to charities in order to

(Continued from previous page) _____

Inc. (Sept. 21, 2015 to present). In nearly every case, Abramovich was the sole incorporator, officer, and director; at a minimum, he controlled each of these companies. The listed addresses for the corporations appear to match residential addresses associated with Abramovich. Thus, as explained more fully in paragraph 27, hereinafter, all references to Abramovich include Mr. Abramovich, personally, and the companies that he owns or controls.

³ 47 U.S.C. § 227(e).

⁴ 47 CFR § 64.1604.

⁵ *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 18 FCC Rcd 14014, 14122, para. 179 (2003).

⁶ *Id.*

⁷ 47 U.S.C. § 227(e).

⁸ See 156 Cong. Rec. H2522, H2524 (2010) ("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.").

⁹ *Id.* at H2525.

misappropriate donations.¹⁰ Such scams and frauds were precisely the types of activities that Congress had in mind when it adopted the Truth in Caller ID Act.¹¹

B. FCC Investigation into Abramovich’s Spoofed Robocalls

5. In recent years, consumers have reported receiving spoofed robocalls offering vacation packages, including to Mexico and the Caribbean. The calls appear as local numbers on caller ID systems, often tricking consumers into answering.¹² When consumers answer the call, they hear a prerecorded message instructing them to “Press 1” to hear more about an “exclusive” vacation deal offered by a well-known travel or hospitality company such as TripAdvisor, Expedia, Marriott, or Hilton. Consumers are then transferred to a call center, where live operators attempt to sell the consumer one or more vacation packages (usually involving timeshare presentations), but are not affiliated with the well-known and trusted brands presented to the consumer during the prerecorded message. Some consumers report receiving these calls multiple times per week.¹³

6. In December 2015, Spök, Inc. (Spök) contacted the Commission to report and complain about a significant robocalling event that was disrupting its emergency medical paging service. Spök, headquartered in Springfield, Virginia, provides paging services for hospitals, emergency rooms, and physicians. Paging services are essential in hospitals and emergency rooms across the country, with an estimated 85 percent of hospitals relying on this technology to ensure that emergency room doctors, nurses, EMTs, and other first responders receive immediate alerts.¹⁴ Because paging technology is not equipped to handle voice calls, a large-scale robocalling campaign will disrupt—and can potentially disable—the network. Service outages, slowdowns, or other problems caused by robocalls flooding a paging network constitute a serious risk to public safety because they interfere with critical hospital and emergency room communications. From the information provided by Spök, the Commission traced the calls to Adrian Abramovich through his company, Marketing Strategy Leaders, Inc., a Florida based corporation.¹⁵

7. In April 2016, TripAdvisor, Inc.¹⁶ contacted the Bureau to report that it had received a number of consumer complaints about robocalls that invoked the TripAdvisor name without

¹⁰ 156 Cong. Rec. H8376, H8380 (2010).

¹¹ See 156 Cong. Rec. H2522, H2523 (2010) (“Caller ID spoofing has emerged as a useful tool for identifying thieves and other scam artists.”).

¹² As part of the investigation, Enforcement Bureau staff spoke with consumers who confirmed these same sentiments, namely extreme frustration and annoyance about these spoofed calls. One consumer said she uses her cellular phone for business and cannot afford to not pick up a local call because it might be a client or business lead. These robocalls distract her from her work and waste her time. Declaration of Daniel Stepanicich, February 13, 2017 (on file in File No. EB-TCD-15-00020488) at 11 (Declaration of Daniel Stepanicich).

¹³ See Zendesk Complaint #1370065 (Dec. 28, 2016); Zendesk Complaint #1364829 (Dec. 22, 2016); Zendesk Complaint #1330923 (Nov. 2016); Zendesk Complaint #1297041 (Nov. 1, 2016); see also *infra* para. 13.

¹⁴ See *Hospitals turning a ‘pager’ on data hardware*, The Boston Globe (Feb. 2, 2016), <https://www.bostonglobe.com/business/2016/02/01/beep-this-accessory-busy-doctors-finally-gets-upgrade/gRcjTy7w3RuTJiqaeKTsEN/story.html>.

¹⁵ According to the Florida Secretary of State corporate filing web database, Abramovich dissolved Marketing Strategy Leaders on January 29, 2016. The Commission’s investigation, however, found call data records for Marketing Strategy Leaders as recent as December 31, 2016. See Carrier Call Detail Records, January 11, 2017 (on File No. EB-TCD-15-00020488) (Call Detail Records).

¹⁶ TripAdvisor, Inc. (TripAdvisor) is a publicly traded U.S. advice and information company that offers user-generated reviews of travel accommodations, restaurants and tourism attractions. See About TripAdvisor, <https://tripadvisor.mediaroom.com/us-about-us>. TripAdvisor provides a portal for third party travel provider partners to promote their services, but does not itself sell any travel tickets or vacation packages. *Id.* (“TripAdvisor [] is not a booking agent or tour operator, and does not charge any service fees to users of our site.”).

TripAdvisor's knowledge or authorization. Specifically, consumers reported receiving unwanted calls with prerecorded messages claiming to be on behalf of TripAdvisor.¹⁷ In response to these complaints, TripAdvisor launched an independent investigation and determined that the robocalls directed consumers to various websites purporting to be travel companies.¹⁸ Furthermore, TripAdvisor's investigation found that these travel companies contracted with Abramovich's Marketing Strategy Leaders to place the robocalls.¹⁹

8. Both TripAdvisor and the Commission found evidence of common control of the various travel companies including identical webpage content, shared web hosting servers, and shared contact information.²⁰ TripAdvisor's investigator found that these websites are linked to a group of current and former senior executives and managers at the Sunset World Group—a Mexican hotel and resort chain.²¹ Based on the information that TripAdvisor obtained in its investigation, the robocalling scheme works as follows: Abramovich, as the service provider and lead generator, makes robocalls to American and Canadian consumers. When the consumer picks up the phone, expecting it to be from a local caller, he or she hears an advertising message instructing them to "Press 1" to hear more about an "exclusive" vacation deal offered by a well-known travel or hospitality company such as TripAdvisor, Expedia, Marriott, or Hilton. If the robocall recipient presses "1" for more information, then he or she is directed to one of several different travel agencies (such as Holiday Sands International) that have contracted with Abramovich to receive calls generated by his network. In actuality, the travel agencies were working with Mexican-based call centers engaged in selling timeshares and vacation packages to various Mexican timeshare facilities.²²

9. On December 13, 2016, Bureau staff subpoenaed Marketing Strategy Leaders' call records. The carrier responded on January 11, 2017, providing call records covering the three-month period from October 1, 2016 to December 31, 2016.²³ According to subpoena responses received by the Commission, Abramovich, purporting to do business as Marketing Strategy Leaders, made 96,758,223 calls during this time period,²⁴ averaging over a million calls a day.²⁵ Furthermore, Bureau staff sampled

¹⁷ These unauthorized calls caused undue harm to TripAdvisor's brand and reputation in the minds affected consumers. In one complaint, a consumer appeared particularly outraged that "TripAdvisor" was contacting them:

I JUST RECEIVED AN UNSOLICITED ROBOCALL TO MY PERSONAL PHONE NUMBER THAT IS ON A DO NOT CALL LIST. THAT CALL STATED THAT IT WAS ON BEHALF OF TRIP ADVISORS TRYING TO SELL ME SOMETHING. IF I EVER GET A CALL LIKE THAT AGAIN, I WILL CONTACT THE FCC AND I WILL OPEN THE GATES OF HELL ON TRIP ADVISORS. NEVER NEVER NEVER NEVER CALL ME LIKE THAT AGAIN. EVER. GOT IT. Declaration of [REDACTED], Apr. 4, 2017 (on file in File No. EB-TCD-15-00020488) (Declaration of [REDACTED]).

TripAdvisor did not make the offending robocall. *Id.*

¹⁸ Some of the websites included sunpricevacations.com, pricelesstimes.com, and holidaysandsinternational.com. Declaration of [REDACTED].

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

²³ See Call Detail Records.

²⁴ *Id.* Total calls for each month are as follows: 36,539,979 (October), 30,724,165 (November), and 29,502,000 (December). *Id.*

²⁵ *Id.* On his busiest day, October 19, 2016, Abramovich made 2,121,106 calls. The fewest calls he made on a single business day was 644,051 and averaged over 200,000 calls on Saturdays.

1,000 calls from the call records for each day of the three-month period that Abramovich made calls (for a total sample of 80,000 calls) and found that every reviewed call was spoofed.²⁶ Each calling number was spoofed in order to match the area code (first three digits) and central office code (second three digits) of the called number.²⁷

10. Based on the evidence collected during the investigation, the Bureau cited Abramovich for making illegal robocalls in violation of the Telephone Consumer Protection Act (TCPA) and for committing wire fraud.²⁸ Those violations are separate from, and in addition to, the apparent spoofing violations set forth in this NAL.

III. DISCUSSION

11. We find that Abramovich apparently violated Section 227(e) of the Act and Section 64.1604 of the Rules by causing the display of misleading or inaccurate caller ID information, or “spoofing,” with unlawful intent, for the purpose of aiding an illegal robocalling campaign. Section 227(e) of the Act and Section 64.1604 of the Rules prohibit any person within the United States, in connection with any telecommunications service or Internet Protocol-enabled voice service, to knowingly cause, directly or indirectly, any caller ID service to transmit or display misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value.²⁹

A. Abramovich Apparently Knowingly Caused the Display of Misleading and Inaccurate Caller ID Information

12. Abramovich apparently knowingly caused the display of inaccurate caller ID information. Call records obtained from Abramovich’s carrier show that between October 2016 and December 2016, Abramovich made 96,758,223 robocalls.³⁰ The call records contained the called number, caller ID number, time stamp, call duration, and the IP address that sent the calls to the carrier. As stated above, Bureau staff analyzed a representative sample of the calls from the call records for each day during October, November, and December 2016 and found that the first six digits of each caller ID number matched the first six out of ten digits of the called consumer—a practice often referred to as “neighbor spoofing.”³¹ Neighbor spoofing, without question, results in the display of inaccurate caller ID information. Therefore, based upon the large sample reviewed by Bureau staff, we find that Abramovich apparently knowingly caused the display of inaccurate caller ID information in violation of the Act and the Rules.

13. The spoofed caller ID was also misleading. Neighbor spoofing misleads consumers into thinking they are receiving a local call. Numerous consumers complained to the Commission about Abramovich’s use of neighbor spoofing. For example:

- Over the past two weeks, I have received a phone call from a number with the same area code and first three digits of my own.³²

²⁶ See Reviewed Carrier Call Detail Records (on File EB-TCD-15-00020488) (Reviewed Carrier Call Detail Records).

²⁷ *Id.*

²⁸ See Abramovich Citation.

²⁹ 47 U.S.C. § 227(e); 47 CFR § 64.1604.

³⁰ See *supra* para. 9-10.

³¹ See *id.* “Neighbor spoofing” involves altering the caller ID information to mimic the first six digits—the area code and central office code—of the called number.

³² Zendesk Complaint #1295430 (Oct. 31, 2016).

- I have received repeated pre-recorded messages, some claiming to be from Marriott . . . they keep spoofing different numbers.³³
- I have daily—sometimes multiple times [a] day—inbound spoofed calls (same area code and prefix as my own phone number) purporting to be from [Marriott]. . . .³⁴
- I’m on the do-not-call list, and I get telemarketing robo-calls to my cell phone every two hours. It’s unbelievably infuriating. All of them have my same area code (617) and middle code (284) but the last 4 digits change every time.³⁵

14. Based upon the evidence, we find that Abramovich apparently knowingly caused the display of inaccurate or misleading caller ID information. This action, combined with the requisite intent (discussed below), violates Section 227(e)(1) of the Act and Section 64.1604(a) of the Rules.

B. Abramovich’s Falsification of Caller ID Was Done With the Apparent Intent to Defraud, Cause Harm, or Wrongfully Obtain Something of Value

15. Section 227(e) of the Act and Section 64.1604 of the Rules prohibits “in connection with any telecommunications service or IP-enabled voice service” the display of misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value.³⁶ In this instance, Abramovich apparently knowingly spoofed caller ID information with the intent to perpetuate an illegal robocalling campaign that was harmful to both consumers and businesses and in violation of the federal wire fraud statute.

16. Intent to Cause Harm. It is unlawful to display misleading or inaccurate caller ID information when the caller’s purpose or intent for doing so is to cause harm. 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.”³⁷ Both Congress and the Commission have long recognized the unique threats posed by illegal robocalls, including that such calls are a nuisance and invasion of privacy.³⁸ Similarly, courts have routinely recognized that robocalls are an invasion of privacy, an injury in fact sufficient for Article III jurisdiction.³⁹ Spoofing deceptively enhances the efficacy of illegal robocalling campaigns by attempting to trick consumers into answering the call and trusting the caller. In addition to the harms caused by illegal robocalls generally, Abramovich’s spoofing campaign poses additional harms. In this case, Abramovich apparently intended to spoof millions of calls in order to perpetuate an illegal robocalling campaign, which is an inherently harmful practice.

³³ Zendesk Complaint #1298563 (Nov. 2, 2016).

³⁴ Zendesk Complaint #1330923 (Nov. 28, 2016).

³⁵ Zendesk Complaint #1364829 (Dec. 22, 2016).

³⁶ 47 U.S.C. § 227(e); 47 CFR § 64.1604.

³⁷ Truth in Caller ID Order, 26 FCC Rcd at 9122, para 22.

³⁸ See Pub. L. No. 102-243 (1991); *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 7 FCC Rcd 8752 (1992).

³⁹ See, e.g., *Frisby v. Schultz*, 487 U.S. 474, 484 (1988) (recognizing that preserving the sanctity of the home is an important value); *Mims v. Arrow Financial Services, LLC*, 565 U.S. 368, 372 (2012) (finding that robocalls are an invasion of privacy); *LaVigne v. First Community Bancshares, Inc.*, 2016 WL 6305992 at *4 (D.N.M. Oct. 9, 2016) (finding that the invasion of privacy is a concrete harm); *Krakauer v. Dish Network LLC*, 168 F.Supp.3d 843, 845 (M.D.N.C. 2016) (holding that violations of the TCPA are concrete injuries because unwanted telemarketing calls are “a disruptive and annoying invasion of privacy”).

17. *Harm to Consumers.* The spoofed calls appeared to originate from local numbers. Consumers reported frustration at being tricked into answering the calls and explained that they feel powerless to effectively block the unwanted calls because the spoofed numbers constantly change.⁴⁰

18. “Neighbor spoofing” also harms the true subscriber of the spoofed number when affected consumers redial the spoofed number, thinking they are dialing the telemarketer, and instead reach the neighbor. For example, in one instance a consumer left multiple voicemail messages with the true subscriber demanding they stop the calls.⁴¹ Other consumers have reported similar experiences:

- I received an angry telephone call today from a man who says that my cell phone number has been calling him frequently with a Marriott prerecording about reservations.⁴²
- My phone number/caller ID is coming up on someone else’s number. The gentleman called me to inform me that my number/caller ID shows up on his phone and when he answers it’s Marriott Telemarketing.⁴³
- I am getting calls from people whom I don’t know, telling me they are receiving calls from my number saying that someone keeps calling them trying to sell them services from Marriott Corporation. I am not calling them, and I have no ID [sic] who this corporation is.⁴⁴

19. *Harm to Carriers.* Extensive illegal robocalling can overwhelm a network’s capacity, and spoofing makes it harder for carriers to detect those calls and take remedial action. Neighbor spoofing in particular is a technique that robocall scammers use to evade detection by the carriers’ network fraud prevention systems; because the illegal traffic masquerades as normal call traffic between local end users it is more likely to evade detection by carriers or consumers. Spoofed robocalls harm telecommunications carriers by (1) burdening the carriers’ networks with illegal calls, and (2) enraging consumer recipients of the illegal robocalls—whose complaints add to the workload of customer service agents, decrease the perceived value of the service, and increase carrier costs. The harder it is to detect the source of the calls, the longer these harms persist and the more damage they inflict.

20. *Harm to Misrepresented Companies.* Abramovich’s spoofed robocalls harmed the companies mentioned in the robocall messages. Consumers believed that the calls were coming from Marriott or TripAdvisor and threatened to cease doing business with them.⁴⁵ Some consumers have complained on online forums, further tarnishing their goodwill to a wider audience.⁴⁶ By masking the originating number, spoofing makes it harder to identify the perpetrators of illegal robocalling campaigns. The longer it takes to detect the source of the calls, the more damage can be done to the companies’ reputations.

21. In just the last three months of 2016, Abramovich made nearly 100 million apparently illegal spoofed calls, disrupting and angering consumers.⁴⁷ Whereas unspoofed telemarketing calls can be

⁴⁰ *Id.*

⁴¹ Zendesk Complaint #1028233 (June 9, 2016).

⁴² Zendesk Complaint #1473554 (Feb. 24, 2017).

⁴³ Zendesk Complaint #1482115 (Mar. 1, 2017).

⁴⁴ Zendesk Complaint #1420686 (Jan. 27, 2017).

⁴⁵ *See supra* para. 7, note 17.

⁴⁶ *See john_thai, Robo calls??* (June 28, 2016), <https://www.rewards-insiders.marriott.com/thread/48697> (“I usually don’t spout off when I get angry. Time for an exception. Dear Marriott Insiders. Talk to your boss. I just got a robo-call from Marriott on my cell phone. It’s on the no call list and I’ve never given you permission to call me. Do it again and you lose a Lifetime Platinum customer. I didn’t buy a phone in order to provide you with a marketing platform. STOP IT!”).

⁴⁷ *See* Abramovich Citation.

ignored by consumers using caller ID and call blocking services, Abramovich's spoofed telemarketing calls—masquerading as local numbers—trick consumers into answering the phone for fear of missing a call from a neighbor, family member, childcare provider, or business client only to be subjected to an unwanted prerecorded sales message.⁴⁸ This is disruptive and an invasion of privacy, and precisely the type of harmful conduct that Congress sought to prevent via the Truth in Caller ID Act. Moreover, spoofing of this particular variety allows illegal robocalls to propagate undetected from carrier to carrier, adding unauthorized burdens to carrier networks and threatening the integrity of the nation's telecommunications infrastructure. Finally, misrepresenting that the calls were associated with well-known travel and hospitality companies harmed those companies' reputations, and the spoofing made the calls harder to detect and prevent. Based on the representative sample of calls investigated during the three-month period at the end of 2016, we conclude that Abramovich apparently made 96,758,223 spoofed telemarketing robocalls with the intent to causing harm, defraud, or wrongfully obtain something of value.

C. Proposed Forfeiture

22. Section 227(e) of the Act and the Section 1.80 of the Rules authorize the Commission to impose a forfeiture against any person that engages in unlawful spoofing.⁴⁹ Specifically, the Act and Rules authorize a forfeiture of up to \$11,052 for each spoofing violation, or three times that amount for each day of a continuing violation, up to a statutory maximum of \$1,105,241 for any single act or failure to act.⁵⁰ The Truth in Caller ID Act empowers the Commission “to proceed expeditiously to stop and . . . assess a forfeiture penalty against, any person or entity engaged in prohibited caller ID spoofing without first issuing a citation” against the violator.⁵¹

23. This is the first time that the full Commission has proposed a forfeiture for spoofing under the Truth in Caller ID Act. While the Act and Section 1.80 of the Rules set a maximum forfeiture

⁴⁸ Declaration of Daniel Stepanicich at 10-11.

⁴⁹ 47 U.S.C. § 227(e)(5); 47 CFR § 1.80(b)(4). The Truth in Caller ID Act and the 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. As a result, the Bureau is not required to demonstrate the “conscious and deliberate commission or omission of any act” or that such act happened more than once or for more than one day to propose a forfeiture for apparently unlawful spoofing. See 47 U.S.C. §§ 312(f)(1)-(2) (defining “willful” and “repeated” under the Act). We nevertheless find that Abramovich willfully and repeatedly spoofed caller ID information with the intent to harm.

⁵⁰ See 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). See *Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, DA 16-1453, (Dec. 30, 2016).

⁵¹ Truth in Caller ID Order, 26 FCC Rcd at 9132-33, para. 47. Under Section 503(b)(5) of the Act, a person who does not hold a license, permit, certificate, or other authorization issued by the Commission, or is not an applicant for the same, may not be issued a Notice of Apparent Liability for Forfeiture unless: (1) that person is first sent a citation of the violation charged, (2) is given an opportunity for a personal interview with an official of the Commission, and (3) subsequently engages in conduct of the type described in such citation. 47 U.S.C. § 503(b)(5). By contrast, the Truth In Caller ID Act only requires that the Commission provide the notice required under Section 503(b)(3) of the Act (notice and opportunity for a hearing before the Commission or an administrative law judge) or Section 503(b)(4) of the Act (Notice of Apparent Liability for Forfeiture) before assessing a forfeiture for unlawful spoofing. 47 U.S.C. § 227(e)(5)(A). Here, we provide the required notice under Section 503(b)(4) of the Act through this Notice of Apparent Liability for Forfeiture.

amount, the Commission has not previously considered how to calculate proposed forfeitures for spoofing.⁵²

24. When adopting its spoofing rules, the Commission said that it would “seek substantial penalties” against violators.⁵³ Because of the ease and low costs that technology has brought to the task of generating telephone calls and falsifying caller ID information for unlawful purposes, large-scale violators may generate hundreds of thousands or even millions of illegal calls within a short period of time. We find that large-scale spoofing operations tend to be more harmful to consumers. A single spoofed call every month or so is an annoyance, a spoofed call every day is disruptive, and multiple spoofed calls each day can be harassing and even cause consumers to cancel phone service altogether. Even where consumers do not receive multiple spoofed calls, sending spoofed calls to thousands or millions of consumers increases the scope of harm, and in this instance, has increased the damage to upstanding businesses deceptively associated with these calls. Accordingly, any proposed forfeitures in such cases must reflect the exponential harm associated with large-scale spoofing operations where the spoofer has the intent to defraud, cause harm, or wrongfully obtain something of value. At the same time, we recognize that in cases involving massive spoofing campaigns, there is a risk that the fine will far exceed any person or company’s ability to pay.

25. In this case, we calculate the proposed forfeiture to account for the egregiousness of the harm caused by this massive spoofing activity and to serve as both a punishment and a deterrent to future wrongdoing. Nevertheless, we recognize that this is a case of first impression.⁵⁴ Consistent with prior precedent in such cases of first impression, we propose a per violation amount at a level well below the maximum in recognition of the fact that we have not previously proposed a forfeiture for this particular kind of violation, but that will still serve to put bad actors on notice that we take such violations seriously and will act as a deterrent to other large scale spoofing operations. Consistent with prior instances in which we have not previously proposed forfeiture amounts for a particular type of violation,⁵⁵ we propose a base forfeiture in the amount of \$1,000 per unlawful spoofed call.⁵⁶ We will then multiply the base forfeiture value of \$1,000 to each of the 80,000 calls that the Commission specifically examined that apparently involved unlawful caller ID spoofing, for a total base forfeiture of \$80,000,000 for which Abramovich is apparently liable.⁵⁷

⁵² See 47 U.S.C. § 227(e) (setting a statutory maximum at \$10,000 per violation); 47 CFR § 1.80 (adopting the statutory maximum with the required inflation adjustment); *Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, DA 16-1453 (Dec. 30, 2016).

⁵³ Truth in Caller ID Act Order, 26 FCC Rcd at 9114, para. 2.

⁵⁴ We will evaluate proposed forfeiture amounts in future spoofing cases in light of their particular facts and circumstances, in accordance with Section 503, including notice of the Commission’s intention to act quickly and effectively to deter flagrant misconduct. 47 U.S.C. § 503.

⁵⁵ The Commission took a similar approach in setting the base forfeiture for cramming. See *Long Distance Direct, Inc.*, Notice of Apparent Liability for Forfeiture, 14 FCC Rcd 314 (1998); see also *Onelink Communications, Inc.*, *TeleDias Communications, Inc.*, Notice of Apparent Liability for Forfeiture, 31 FCC Rcd 1403, 1419, para. 28 (2016); *Norristown Telephone Company, LLC*, Notice of Apparent Liability for Forfeiture, 26 FCC Rcd 8844, 8850, paras. 21-22 (2011). The Rules did not provide guidance for calculating forfeitures for cramming, but the Commission determined that cramming was akin to slamming—which had a base forfeiture amount—because both involved misleading consumers. *Long Distance Direct, Inc.*, 14 FCC Rcd at 336-337, para. 29.

⁵⁶ 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 example) to the statutory maximum (misrepresentation/lack of candor). Because there are no directly analogous violations covered within the existing range of base forfeitures, we find that establishing the base forfeiture amount of \$1,000 is reasonable as applied to the specific facts in this case.

⁵⁷ FCC staff confirmed that the 80,000 calls examined involved apparent spoofing but the actual number of spoofed calls, even during this limited period, appears to be likely higher. See Reviewed Carrier Call Detail Records

(continued....)

26. In addition to the base forfeiture proposed above, we find that the circumstances in this case merit a significant upward adjustment. The sheer volume of calls that Abramovich made—96,758,223 calls between the period of October 1, 2016 and December 31, 2016⁵⁸—illustrates that Abramovich’s violations are egregious in number. Likewise, the direct harms from Abramovich’s illegal robocalling campaign are so egregious that that an upward adjustment is warranted.⁵⁹ Furthermore, Abramovich is highly culpable. The call records show that the calls were made by Marketing Strategy Leaders—a company solely owned by, and sharing the residential address of, Adrian Abramovich. Additionally, this is not Abramovich’s first experience with the Communications Act. In 2007, AT&T Mobility received a consent judgment and permanent injunction against Abramovich for unlawful telemarketing calls in violation of the TCPA.⁶⁰ Therefore, after applying the statutory factors, we propose an upward adjustment, to the base forfeiture established above, of \$40,000,000. Thus, the total proposed forfeiture for which Abramovich is apparently liable is \$120,000,000.

27. Additionally, we propose to hold Adrian Abramovich directly liable for the total forfeiture. The Commission may pierce the corporate veil to “prevent reliance on [the] corporate form to frustrate our efforts to implement core statutory provisions.”⁶¹ 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 corporation and the individual no longer have separate personalities, and (2) an inequity will result if the acts are treated to the corporation alone.⁶² Piercing the corporate veil, however, is only relevant if the corporate entity actually exists.⁶³ Here, Adrian Abramovich dissolved Marketing Strategy Leaders on January 21,

(Continued from previous page) _____

(spreadsheet identifying the 80,000 call detail records reviewed by Bureau staff). Even though we limit the total number of violations here to the 80,000 calls verified, we reserve the right in the future, especially with large scale spoofing operations, to use the total number of calls made where there is a high likelihood of violations based on the use of a representative sampling of calls.

⁵⁸ See 47 U.S.C. § 503(b)(4) (“[N]o forfeiture penalty shall be imposed under this subsection against any person unless and until . . . the Commission issues a notice of apparent liability, in writing, with respect to such person. [. . .] Such a notice shall (i) identify each specific provision, term, and condition of any Act, rule, regulation, order, treaty, convention, or other agreement, license, permit, certificate, instrument, or authorization which such person apparently violated or with which such person apparently failed to comply; (ii) set forth the nature of the act or omission charged against such person and the facts upon which such charge is based; and (iii) state the date on which such conduct occurred.”). For purposes of this NAL, we take action only with respect to those violations occurring within the three-month period identified above. See Call Detail Records; Reviewed Carrier Call Detail Records; *Purple Communications, Inc.*, Forfeiture Order, 30 FCC Rcd 14892, 14899-900, paras. 21-23 (2015) (stating that the notice requirements of Section 503 are satisfied when the Notice of Apparent Liability identifies the conduct resulting in the violations and provides “(1) specific cite references to the record (i.e., specific citations to files and documents provided by the violator that identified relevant dates sufficient to allow the violator to lodge its defense) or, (2) citations to the records containing dates and other relevant information”). *Id.* at 14899, para. 22.

⁵⁹ See *supra* paras. 16-20.

⁶⁰ *AT&T Mobility v. Hispanic Solutions*, No. 1:06 cv 02695-WSD (N.D. Ga. Oct. 25, 2007).

⁶¹ *Telseven, LCC, Patrick Hines*, Forfeiture Order, 31 FCC Rcd, 1629, 1635 (2016). See *United States Through Small Business Admin. v. Pena*, 731 F.2d 8, 12 (D.C. Cir. 1984) (quoting *Capital Tel. Co., Inc. v. FCC*, 498 F.2d 734, 738 & n.10 (D.C. Cir. 1974)) (“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.”); *General Tel. Co. of Southwest v. United States*, 449 F.2d 846, 855 (5th Cir. 1971).

⁶² *NLRB v. West Dixie Enterprises, Inc.*, 190 F.3d 1191, 1194 (11th Cir. 1999). 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).

⁶³ *Labadie Coal Co. v. Black*, 672 F.2d 92, 95 (D.C. Cir. 1982).

2016.⁶⁴ Despite formally dissolving Marketing Strategy Leaders, he continued to make spoofed robocalls using the corporate name.⁶⁵ Because Marketing Strategy Leaders ceased to exist by the time of the violations cited in this NAL, Adrian Abramovich is not entitled to the protections of the corporate form and is personally liable for the full forfeiture amount. We also propose holding Marketing Strategy Leaders and Marketing Leaders jointly and severally liable with Adrian Abramovich.⁶⁶ Adrian Abramovich has a practice of quickly forming and closing companies for which he is the sole owner, controller, and officer—Marketing Strategy Leaders and Marketing Leaders are no exceptions.⁶⁷ Accordingly, out of an abundance of caution, we hold both Adrian Abramovich and his companies, Marketing Strategy Leaders, Inc. and Marketing Leaders, Inc., jointly and severally liable for the obligations proposed by this NAL.

IV. CONCLUSION

28. We have determined that Adrian Abramovich apparently willfully and repeatedly violated Section 227(e) of the Act and Section 64.1604 of the Rules. We have further determined that Adrian Abramovich, Marketing Strategy Leaders, and Marketing Leaders are apparently jointly and severally liable for a forfeiture in the amount \$120,000,000.

V. ORDERING CLAUSES

29. **IT IS ORDERED** that, pursuant to Sections 227(e)(5)(A)(i) and 503(b) of the Act⁶⁸ and Sections 1.80 of the Rules,⁶⁹ Adrian Abramovich, Marketing Strategy Leaders, Inc. and Marketing Leaders, Inc. are hereby **NOTIFIED** of this **APPARENT JOINT AND SEVERAL LIABILITY FOR A FORFEITURE** in the amount of one hundred twenty million dollars (\$120,000,000) for willful and repeated violations of Section 227(e) of the Act,⁷⁰ Section 64.1604 of the Rules,⁷¹ and the *Rules and Regulations Implementing the Truth In Caller ID Act of 2009*.⁷²

30. **IT IS FURTHER ORDERED** that, pursuant to Section 1.80 of the Rules,⁷³ within thirty (30) calendar days of the release date of this Notice of Apparent Liability for Forfeiture, Adrian Abramovich, Marketing Strategy Leaders, Inc. and Marketing Leaders, Inc. **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 paragraph 33 below.

31. Payment of the forfeiture must be made by check or similar instrument, wire transfer, or credit card, and must include the NAL/Account Number and FRN referenced above. Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc. shall send electronic notification of

⁶⁴ Articles of Dissolution, Marketing Strategy Leaders, Inc. (Jan. 21, 2016), *available at* <http://search.sunbiz.org/Inquiry/CorporationSearch/ConvertTiffToPDF?storagePath=COR%5C2016%5C0203%5C80058866.Tif&documentNumber=P04000043957>.

⁶⁵ The billing information provided by Abramovich's carrier for October 2016 through December 2016 lists Marketing Strategy Leaders. *See* Call Detail Records.

⁶⁶ *See supra* note 2.

⁶⁷ *Id.*

⁶⁸ 47 U.S.C. §§ 227(e)(5)(A)(i), 503(b).

⁶⁹ 47 CFR § 1.80.

⁷⁰ 47 U.S.C. § 227(e).

⁷¹ 47 CFR § 64.1604.

⁷² *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, Report and Order, 26 FCC Rcd 9114 (2011).

⁷³ 47 CFR § 1.80.

payment to Lisa Williford at Lisa.Williford@fcc.gov on the date said payment is made. Regardless of the form of payment, a completed FCC Form 159 (Remittance Advice) must be submitted.⁷⁴ When completing the FCC Form 159, enter the Account Number in block number 23A (call sign/other ID) and enter the letters “FORF” in block number 24A (payment type code). Below are additional instructions that should be followed based on the form of payment selected:

- Payment by check or money order must be made payable to the order of the Federal Communications Commission. Such payments (along with the completed Form 159) must be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank – Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.
- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. To complete the wire transfer and ensure appropriate crediting of the wired funds, a completed Form 159 must be faxed to U.S. Bank at (314) 418-4232 on the same business day the wire transfer is initiated.
- Payment by credit card must be made by providing the required credit card information on FCC Form 159 and signing and dating the Form 159 to authorize the credit card payment. The completed Form 159 must then be mailed to Federal Communications Commission, P.O. Box 979088, St. Louis, MO 63197-9000, or sent via overnight mail to U.S. Bank – Government Lockbox #979088, SL-MO-C2-GL, 1005 Convention Plaza, St. Louis, MO 63101.

32. 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 20554.⁷⁵ 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.

33. 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 Rules.⁷⁶ 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 Kristi Thompson, Deputy Division Chief, Telecommunications Consumers Division, at Kristi.Thompson@fcc.gov.

34. The Commission will not consider reducing or canceling a forfeiture in response to a claim of inability to pay unless the petitioner submits: (1) federal tax returns for the most recent three-year period; (2) financial statements prepared according to generally accepted accounting practices; or (3) some other reliable and objective documentation that accurately reflects the petitioner’s current financial status. Any claim of inability to pay must specifically identify the basis for the claim by reference to the financial documentation.

⁷⁴ An FCC Form 159 and detailed instructions for completing the form may be obtained at <http://www.fcc.gov/Forms/Form159/159.pdf>.

⁷⁵ See 47 CFR § 1.1914.

⁷⁶ 47 CFR §§ 1.16, 1.80(f)(3).

35. **IT IS FURTHER ORDERED** that a copy of this Notice of Apparent Liability for Forfeiture together with the Reviewed Carrier Call Detail Records shall be sent by first class mail and certified mail, return receipt requested, to Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc. at [REDACTED].

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

**STATEMENT OF
CHAIRMAN AJIT PAI**

Re: *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, File No. EB-TCD-15-00020488.

Have you ever gotten a call in which the phone number looks pretty familiar? The area code matches yours, and the first three “prefix” numbers match yours, but you can’t quite tell who it is?

If so, you’re not alone. This often results from a tactic known as “neighbor spoofing,” and inveterate robocallers are using it to bombard the American people with illegal robocalls without getting caught. Neighbor spoofing often tricks consumers into answering, since they think that the person on the other end must be someone from his or her local community.

Robocalling is consistently the top-ranked category of complaints that consumers bring to the FCC. That’s why I’m pleased that today the Commission is taking major, unprecedented action against what appears to be the most egregious “neighbor spoofing” robocalling scheme we have ever seen. Adrian Abramovich, through several faux marketing companies he owns and manages, appears to have made 96,758,223 robocalls between October 1, 2016 and December 31, 2016. 96,758,223. That works out to over one million unwanted calls every day and almost 44,000 such calls each hour.

Today, we respond in kind, proposing to fine Mr. Abramovich \$120 million.

Mr. Abramovich’s scheme apparently works like this. Upon answering a call, consumers are typically offered what appears to be an “exclusive” vacation deal offered by a well-known travel or hospitality company, like TripAdvisor, Expedia, Marriott, or Hilton. Consumers are prompted to “Press 1” and are then transferred to a call center, where live operators give them the hard sell on low-quality vacation packages that have no relation to the companies previously referenced. Unfortunately, many unsuspecting Americans are deceived into taking the bait.

Make no mistake: Mr. Abramovich appears to have been no passive party to this scam. He apparently found it profitable to send to these live operators the most vulnerable Americans—typically the elderly—to be bilked out of their hard-earned money. Many consumers spent from a few hundred up to a few *thousand* dollars on these “exclusive” vacation packages.

This scheme was particularly abhorrent because, given its breadth, it appears to have substantially disrupted the operations of an emergency medical paging provider. It did this by slowing down and potentially disabling its network. Pagers may be low-tech, but for doctors, these devices are simple and dependable standbys. By overloading this paging network, Mr. Abramovich could have delayed vital medical care, making the difference between a patient’s life and death.

Thanks to the tenacious sleuthing by the staff of our Enforcement Bureau, we were able to connect the dots among numerous consumer complaints that showed us the scope of Mr. Abramovich’s apparent scheme. The Bureau hand-verified over 80,000 calls from this three-month period. Every single one was spoofed to show what consumers must have thought was a local number. The Bureau also interviewed several people who had received calls, none of whom had provided consent.

Today marks the first time that the FCC is taking enforcement action against a large-scale spoofing operation under the Truth in Caller ID Act. This FCC is an active cop on the beat for consumers, and a cop that means business when it to their top concern: the scourge of robocalls. We aim to put unlawful robocallers out of business and to deter anyone else from hatching a business plan that plunders American consumers’ pocketbooks.

Thank you to the dedicated staff of the Enforcement Bureau, including Vilma Anderson, Tamara Baxter, Michael Carowitz, Lisa Gelb, Richard Hindman, Lisa Landers, Latashia Middleton, Nakasha Ramsey, Stacy Ruffin-Smith, Michael Scurato, Daniel Stepanicich, Kristi Thompson, Kim Thorne, Melanie Tiano, Bridgette Washington, and Lisa Williford for their meticulous work on this investigation.

**STATEMENT OF
COMMISSIONER MIGNON L. CLYBURN**

Re: *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, File No. EB-TCD-15-00020488.

Anyone who has ever contacted the FCC's Washington, DC headquarters is familiar with these six digits: 202-418. Given this association, if that area code and prefix appeared on your caller ID, you would more than likely answer the call (at least I like to think you would). But when phone numbers are spoofed and what appears to be a trusted or familiar source actually originates from a party intent on misleading, defrauding, causing harm, or wrongfully obtaining something of value, we each have a serious and potentially dangerous problem on our hands.

Unwanted robocalls are universally hated. Too often, they disrupt some of our most precious, and increasingly rare moments of peace and quiet. And to say that the case before us, is one of the most troubling that I have ever seen in this context, is one of the biggest understatements I have made in years. One man, a single individual, is apparently responsible for nearly 100 million robocalls during a three month period. Adrian Abramovich's alleged spoofing activities, has had a direct and adverse financial impact on consumers, the reputational harm of respected American businesses and if that were not enough, has been a serious threat to public safety.

During the FCC Enforcement Bureau's review of these apparent spoofed telephone calls, it was discovered that some consumers paid hundreds of dollars for vacations that differed significantly from the ones presented to them. This has caused incalculable harm to well-regarded American travel companies, as their names were misappropriated and their hard-earned reputations were maligned as consumers were misled presumably for financial gain. Mr. Abramovich's apparent robocall spoofing scheme also disrupted an emergency medical paging service designed to ensure that first responders receive immediate critical alerts.

I wish that I could promise the American people that today's action will put an end to all unwanted and as this case makes apparent, dangerous robocalls. Sadly, this Notice of Apparent Liability addresses only a fraction of the approximately 2.6 billion robocalls that YouMail's Robocall Index reports were made just during the month of May. But there is one thing that I know on which we all agree: If there is any case of where a first impression should be lasting, it is this one. I wholeheartedly support being as tough as we can justify, on anyone who would violate the public's trust, intentionally violate the Commission's rules, and put people at risk for apparent personal gain. And a proposed penalty of \$120 million, the largest in the FCC's history, shows just how serious we are in stamping out the largest spoofed robocall campaign we have yet to investigate.

The Commission has an obligation to ensure that all of its rules are robustly enforced, including those that protect consumers against 9-1-1 outages, cramming, slamming, and other core consumer protections. A Commission that is truly committed to putting #ConsumersFirst, must never issue a hall pass to any communications provider that egregiously violates the Truth in Caller ID Act or any of our standing rules.

The American people are counting on us to be the voice that stands against practices that harm competition and limit consumer choice. We have much more work to do when it comes to these goals, but today it pleases me to say, we have taken a noteworthy step.

My thanks to the Enforcement Bureau staff for your extensive work on this item and for your continued efforts to address the Commission's number one consumer complaint: illegal robocalls.