

**Before the
Federal Communications Commission
Washington, DC 20554**

In the Matter of)	
)	
Kenneth Moser dba Marketing Support Systems)	File No.: EB-TCD-18-00028267
)	NAL/Acct. No.: 202032170001
)	FRN: 0029043379

NOTICE OF APPARENT LIABILITY FOR FORFEITURE

Adopted: December 12, 2019

Released: December 13, 2019

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

I. INTRODUCTION

1. Combatting unlawful, unwanted telephone calls—including unlawfully “spoofed” calls—is the top consumer-protection priority of the Federal Communications Commission. Caller ID information is spoofed when caller ID information 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.¹ This Notice of Apparent Liability advances the Commission’s ongoing efforts to crack down on unlawful robocalls by taking action against a particularly egregious spoofing scheme that targeted a business rival and smeared a political candidate while also harming thousands of call recipients with distressing, and factually baseless, messages.

2. Kenneth Moser, doing business as a telemarketing enterprise under the name Marketing Support Systems (Moser), apparently made 47,610 unlawful spoofed calls over the course of a two-day calling campaign.² Moser apparently spoofed the phone number assigned to another telemarketing company, HomeyTel, Inc., (HomeyTel) to transmit a prerecorded voice message containing false statements critical of California State Assembly candidate Philip Graham. Moser is not affiliated with HomeyTel and was not authorized to use its phone number. To the contrary, he has a long and contentious relationship with HomeyTel and that company’s founder and current manager, Conrad Braun. As a result of the spoofed calls, HomeyTel received a multitude of complaints from recipients of the prerecorded voice message call, as well as a cease-and-desist letter from the candidate referenced in the message.

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

² Marketing Support Systems, Document No. 2015-013003, County of San Diego, Recorder/County Clerk (May 14, 2015) (on file in EB-TCD-18-00028267); *see also* Better Business Bureau, *Marketing Support Systems*, <https://www.bbb.org/us/ca/san-diego/profile/telemarketing-services/marketing-support-systems-1126-1014054> (last visited Nov. 18, 2019) (*Marketing Support Systems BBB Profile*); LinkedIn, *Kenneth Moser Profile*, <https://www.linkedin.com/in/kenneth-moser-3199a24> (last visited Nov. 18, 2019). Marketing Support Systems provides telemarketing services, offering “lead generation and marketing campaigns.” *Marketing Support Systems BBB Profile*.

3. We find that Moser apparently violated the Truth in Caller ID Act by making the spoofed calls with the intent to cause harm and wrongfully obtain something of value.³ Given the egregious circumstances, we propose a forfeiture of \$9,997,750.

II. BACKGROUND

4. *Legal Background.* Congress recognized that consumers have 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.⁴ 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[.]”⁵

5. 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 via wireless phones can be costly.⁶ Through the TCPA, Congress provided greater protections for consumers from such calls.⁷ The statute and the Federal Communications Commission’s (Commission or FCC) implementing rules prohibit prerecorded voice message calls to wireless telephone numbers without subscribers’ prior consent—unless made for an emergency purpose,⁸ and mandate inclusion of the telephone number of the entity responsible for initiating the call.⁹ Political campaign-related prerecorded

³ The Bureau is releasing contemporaneously a Citation and Order notifying Moser that, in conjunction with the apparently unlawful spoofing activities, Moser violated the Telephone Consumer Protection Act (TCPA) and the Commission’s rules by (1) making prerecorded message calls to wireless phone numbers without the customers’ consent or an emergency purpose, 47 U.S.C. § 227(b)(1)(A)(iii); 47 CFR § 64.1200(a)(1)(iii), and (2) failing to include the phone number of the entity or person who was responsible for initiating the call, 47 U.S.C. § 227(d)(3)(A); 47 CFR § 64.1200(b)(2). *Kenneth Moser dba Marketing Support Systems*, Citation and Order, DA 19-1250 (EB 2019) (*Moser Citation*).

⁴ 156 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.”); 155 Cong. Rec. S170-02, S173 (2009) (“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.”).

⁵ 47 U.S.C. § 227(e); *see also* 47 CFR § 64.1604. The prohibition does not apply to lawfully authorized investigative, protective, or intelligence activities of a law enforcement agency of the United States, the states, or a political subdivision of a state, or of an intelligence agency of the United States or to activity allowed pursuant to a court order that specifically authorizes the use of caller ID manipulation. 47 CFR 64.1604(b); *see also* 47 U.S.C. § 227(e)(3)(B)(ii); 47 U.S.C. § 227(e)(7). Those exceptions do not apply here.

⁶ *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*). Similarly, courts have routinely agreed that robocalls are an invasion of privacy, an injury in fact sufficient for Article III jurisdiction. *Mims v. Arrow Financial Services, LLC*, 565 U.S. 368, 372 (2012) (finding that robocalls are an invasion of privacy); *Frisby v. Schultz*, 487 U.S. 474, 484 (1988) (recognizing that preserving the sanctity of the home is an important value); *LaVigne v. First Community Bancshares, Inc.*, 215 F. Supp. 3d 1138, 1146-47 (D. NM 2016).

⁷ 47 U.S.C. § 227(b), (d)(3).

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

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

voice message calls are not exempt from these statutory protections.¹⁰ The Commission has found that spoofing, when employed in an unlawful robocalling campaign, can indicate an intent to cause harm.¹¹

6. *Factual Background.* Moser's apparently illegal activity occurred in the midst of a heated campaign season. On May 30 and 31, 2018, approximately one week before California's primary election, thousands of residents of the California 76th State Assembly District in San Diego County received a robocall message that described in graphic detail an alleged sexual assault involving Philip Graham (Graham), one of eight candidates for the open Assembly seat.¹² The allegations in the recorded message, however, had already been disproven by law enforcement; indeed, the San Diego County Sheriff's Department conducted an investigation into the incident and publicly announced by May 29, 2018, that the alleged sexual assault never occurred.¹³

7. Based upon a complaint referred by the California Secretary of State,¹⁴ the Bureau initiated an investigation. Bureau staff traced the robocalls to a third-party dialing platform¹⁵ and

¹⁰ *Biennial Reminder for Political Campaigns About Robocall and Text Abuse, Enforcement Advisory*, 31 FCC Rcd 1940, 1941 (2016); Federal Communications Commission, *Political Campaign Robocalls & Robotexts*, <https://www.fcc.gov/political-campaign-robocalls-robotexts> (last visited Nov. 18, 2019).

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*); *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*).

¹² Jesse Marx, *How a Strange Accusation Caught Fire and Took Down an Assembly Candidate*, Voice of San Diego (Jan. 2, 2019), <https://www.voiceofsandiego.org/topics/politics/how-a-strange-accusation-caught-fire-and-took-down-an-assembly-candidate>. We note that, for purposes of determining that Moser apparently violated section 227(e), we need not, and do not, consider the substantive allegations contained in the prerecorded message.

¹³ San Diego County Sheriff's Department, News Release Information Sheet, rel. May 29, 2018 (on file in EB-TCD-18-00028267); see also Brie Stimson, *Battery Allegations Against Assembly Candidate Phil Graham Unfounded: SDO Investigation*, NBC San Diego (May 29, 2018), <https://www.nbcsandiego.com/news/local/Battery-Allegations-Against-Assembly-Candidate-Unfounded-SDSO-Investigation-484009451.html>. Graham's accuser, Nichole Burgin, was later criminally charged for making a false report of a crime; she pleaded guilty and was sentenced in February 2019. Aaron Burgin, *Burgin to Serve Two Days in Jail for False Accusation Against Phil Graham*, The Coast News (Feb. 5, 2019), <https://www.thecoastnews.com/burgin-to-serve-two-days-in-jail-for-false-accusation-against-phil-graham>. We note that, in California, only the top two vote-getters in a primary election—regardless of party preference—move on to the general election. Graham was the third top vote-getter, losing his bid to move onto the general election. Ballotpedia, https://ballotpedia.org/California_State_Assembly_District_76. Graham's loss, however, is not relevant to our determination that Moser apparently violated section 227(e).

¹⁴ Letter from Steven J. Reyes, Chief Counsel to California Secretary of State, to Rosemary Harold, Chief, FCC Enforcement Bureau et al. (Jun. 2, 2018) (on file in EB-TCD-18-00028267). Reyes forwarded to the Commission a letter and accompanying exhibits from Thomas W. Hiltachk complaining about the robocalls. Letter from Thomas W. Hiltachk, Counsel to State Assembly candidate Philip Graham, to Alex Padilla, California Secretary of State (Jun. 1, 2018) (on file in EB-TCD-18-00028267) (Hiltachk Letter).

¹⁵ Letter from Kristi Thompson, Division Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to [REDACTED] (Nov. 14, 2018) (on file in EB-TCD-18-00028267). The letter also requested a copy of the prerecorded message. The third-party dialing platform, [REDACTED], provides a web-based application that allows customers to make inbound or outbound automated calls. This service allows customers to upload call lists and automated messages and to make associated calls. See also Letter from Kristi Thompson, Division Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to [REDACTED] (Aug. 17, 2018); E-mail from [REDACTED] to Sonja Rifken, Attorney, Telecommunications Consumers Division, FCC Enforcement Bureau (Aug. 21, 2018, 15:32 EDT) ([REDACTED], a company that provides telecommunications services, among others, to [REDACTED] identified [REDACTED] as the third-party dialing platform used to make the calls at issue and Kenneth Moser as the client of [REDACTED] who made the calls.).

discovered that Moser and Marketing Support Systems,¹⁶ a business that provides “lead generation and marketing campaigns,”¹⁷ conducted the robocalling campaign.¹⁸

8. The investigation uncovered that Moser made 47,610 prerecorded voice message calls during the two-day period at issue, including repeated calls to the same recipients.¹⁹ More than 11,000 of those calls were sent to wireless phones in violation of the TCPA’s prohibition on sending prerecorded voice message calls to wireless telephones without the called party’s consent.²⁰ All 47,610 calls failed to include the telephone number of the party responsible for initiating the call, only stating in the prerecorded message that it was “paid for by Jennifer Jones,” an apparent pseudonym.²¹ Moser set the caller ID information for all of the calls he made to display one phone number, 619-223-1022.²² The subscriber of this number is HomeyTel, a company formerly owned and currently managed by Conrad Braun (Braun).²³ Moser is not affiliated with HomeyTel and was not authorized to use its phone number.²⁴

¹⁶ According to [REDACTED], the contact for the account associated with the calls is Marketing Support Systems and owner Kenneth Moser with the address of [REDACTED]. Marketing Support Systems has been registered in San Diego County, California as a “fictitious business name” to Kenneth Moser since 1993 at the same address, although the zip code listed with San Diego County is [REDACTED]. Marketing Support Systems, Document No. 2015-013003, County of San Diego, Recorder/County Clerk (May 14, 2015) (on file in EB-TCD-18-00028267). The state of California permits individuals and partnerships to do business under “fictitious business names,” as defined by California law, provided that the individual or partnership files a “fictitious business name certificate . . . designed to make available to the public the identities of persons doing business under the fictitious name.” Cal. Bus. & Prof. Code § 17900.

¹⁷ *Marketing Support Systems BBB Profile*, <https://www.bbb.org/us/ca/san-diego/profile/telemarketing-services/marketing-support-systems-1126-1014054> (last visited Nov. 18, 2019).

¹⁸ E-mail from [REDACTED], to Parul Desai, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Dec. 12, 2018, 12:38 EST) (on file in EB-TCD-18-00028267) (providing call detail records and certain other relevant information regarding Moser); E-mail from [REDACTED] to Sonja Rifken, Attorney, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 27, 2019, 12:19 EST) (on file in EB-TCD-18-00028267) (updating call records with times of calls) (collectively, Dialing Platform Response).

¹⁹ Dialing Platform Response at Files 6192231022 and Copy of 6192231022 with call times (Call Detail Records).

²⁰ Bureau staff used an industry standard, commercially available software database of known assigned and ported wireless numbers to determine whether any of the robocalls were made to wireless phone numbers. Interactive Marketing Solutions, *EasyID*, <https://www.ims-dm.com/mvc/page/easyid> (last visited Nov. 18, 2019). EasyID is Interactive Marketing Solution’s 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. *Id.*

²¹ Dialing Platform Response at File PHILGRAHAM_REV_VO.MP3 (on file in EB-TCD-18-00028267). Bureau staff has been unable to identify a specific person named “Jennifer Jones” associated with Moser or the robocalls in question.

²² Dialing Platform Response at Call Detail Records and File Response at 5.

²³ E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 8, 2019, 13:52 EST) (on file in EB-TCD-18-00028267) (Declaration of Conrad Braun (Braun Decl.)); *see also* Letter from Kristi Thompson, Division Chief, Telecommunications Consumer Division, FCC Enforcement Bureau, to [REDACTED], to [REDACTED], Senior Analyst, Telecommunications Consumer Division, FCC Enforcement Bureau (Mar. 5, 2019, 9:28 am EST) (on file in EB-TCD-18-00028267) (BNA Response) (confirming that HomeyTel is subscriber).

²⁴ Braun Decl.

9. This is not the first instance in which Moser used HomeyTel's caller ID information to conduct a robocalling campaign.²⁵ On November 3 and 5, 2016, Moser apparently conducted a robocalling campaign and set the caller ID information to show HomeyTel's telephone number. The Commission received one complaint regarding a robocalling campaign on those dates using HomeyTel's telephone number in which the complainant, identified as a San Diego police officer, stated that the "victim [HomeyTel] believes a business rival arranged for an auto-dial system to call hundreds of people using the victim's phone number as the Caller ID number."²⁶ As in 2018, Moser was not authorized to use HomeyTel's phone number in 2016.

10. California court records show that Moser is well acquainted with Braun and HomeyTel. Moser, acting in his individual capacity and using the private right of action provided for in the TCPA, has sued Braun and/or HomeyTel three times over the past several years in small claims court in San Diego County, alleging that Braun and/or HomeyTel violated the TCPA by making "illegal automated phone message [calls] soliciting toner products,"²⁷ "illegal auto dial advertising [calls]"²⁸ and "illegal robo call[s]."²⁹ Moser also claimed that Braun and/or HomeyTel violated the Truth in Caller ID Act in two of these lawsuits.³⁰

11. Moser's familiarity with the relevant law here also is made plain in other legal actions. He has filed or participated in more than a dozen complaints alleging TCPA violations by companies other than HomeyTel.³¹ The allegations in these complaints include Moser's own assertions that TCPA

²⁵ Letter from Kristi Thompson, Division Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to [REDACTED] (Mar. 22, 2019) (on file EB-TCD-18-00028267) (subpoenaing call detail records and certain contact information). [REDACTED] provided the subpoenaed information to the Bureau on March 25, 2019. Email from [REDACTED], to Parul Desai, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Mar. 25, 2019, 16:17 EDT) (on file EB-TCD-18-00028267) (Second Dialing Platform Response). [REDACTED] confirmed that Moser was the contact listed for that account in November 2016. *Id.* See also email from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney, Telecommunications Consumers Division, FCC Enforcement Bureau (Mar. 28, 2019, 22:21 EDT) (on file EB-TCD-18-00028267) (Conrad Braun Supplemental Declaration (Braun Supplemental Decl.) stating that neither Moser nor Marketing Support Systems was authorized to use the HomeyTel number in November 2016.).

²⁶ Zendesk Complaint #1307215 (Nov. 3, 2016) (on file in EB-TCD-18-00028267).

²⁷ *Moser v. Braun et al.*, Case No. 37-2008-00004053-SC-SC-CTL (filed May 29, 2008) (awarding Moser \$1,000 in damages for TCPA violations) (2008 *Moser TCPA*).

²⁸ *Moser v. HomeyTel et al.*, Case No. 37-2012-00005170-SC-SC-CTL (filed Aug. 29, 2012) (voluntarily dismissing HomeyTel from the suit prior to its conclusion) (2012 *Moser TCPA*).

²⁹ *Moser v. Braun*, Case No. 37-2015-00322367-SC-SC-CTL (filed Jun. 8, 2015) (awarding no damages to Moser) (2015 *Moser TCPA*).

³⁰ 2008 *Moser TCPA* (alleging TCPA Truth in Caller ID violations, HomeyTel voluntarily dismissed by Moser) and 2012 *Moser TCPA* (alleging fraud, breach of settlement, and TCPA violations). Braun has also brought countersuit against Moser. *Braun v. Moser*, Case No. 37-2013-00041628-CU-FR-CTL (filed Jun. 13, 2013) (2013 *Braun*). This case is ongoing.

³¹ *E.g.*, *Moser v. Lifewatch, Inc.*, Case No. 37-2019-00024879-SC-SC-CTL (filed Apr. 29, 2019) (case pending); *Moser v. Alliance Security, Inc.*, Case No. 37-2017-00351345-SC-SC-CTL (filed Jul. 12, 2017) (voluntary dismissal by Moser); *Moser v. Quality Credit, LLC*, Case No. 37-2016-00332616-SC-SC-CTL (filed Jan. 5, 2016) (awarding Moser \$2,500 in damages for TCPA violations); *Meyer, Moser v. Capital Alliance Group et al.*, Case No. 15-CV-2405-WVG (S.D. CA filed Oct. 23, 2015) (joint voluntary dismissal); *Engle, Moser v. Unified Life Insurance Co., Inc.*, *et al.*, Case No. 14-CV-1908-MMA-JLB (S.D. CA filed Aug. 13, 2014) (joint voluntary dismissal).

violations cause harm, including harm from the “aggravation and consequent health effects of stress these illegal intrusions have caused.”³²

III. DISCUSSION

12. The Bureau’s investigation indicates that Moser’s activities appear to violate the Truth in Caller ID Act. He apparently knowingly displayed misleading or inaccurate caller ID information. Evidence shows that Moser appears to have intended to cause harm to HomeyTel’s reputation and goodwill by displaying that company’s phone number and thereby lead consumers to believe the calls came from HomeyTel. Moser also appears to have intended to cause harm to recipients of the spoofed calls by subjecting them to an illegal robocalling campaign, something he acknowledges to cause harm. In addition, by hiding behind a false caller ID, Moser intended to wrongfully obtain something of value. Moser used spoofed caller ID in conjunction with an unlawful (i.e., wrongful) robocalling campaign.³³ In so doing, he sought to avoid law enforcement and private TCPA lawsuits. And Moser was compensated for the calling campaign. We thus determine that Moser is apparently liable for violation of section 227(e) of the Act and section 64.1604 of the Commission’s rules.

13. We propose a forfeiture in the amount of \$9,997,750. We calculate the proposed forfeiture by assessing a proposed base forfeiture of \$1,000 per each apparently unlawful call. As we have in other mass-spoofing cases and for pragmatic reasons, 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 5,713 apparently unlawful spoofed calls, yielding a base forfeiture of \$5,713,000. We then adjust the proposed amount to reflect the egregiousness of the specific facts here. In this case, we upwardly adjust the proposed forfeiture by 75%.

A. Moser Apparently Knew That He Was Using Inaccurate Caller ID Information

14. The Truth in Caller ID Act prohibits a caller from knowingly transmitting misleading or inaccurate caller ID information. The Bureau’s investigation revealed that Moser’s May 2018 robocalling campaign apparently met this requirement. The investigation revealed that Moser set the caller ID information to display 619-223-1022 through the third-party dialing platform he used to transmit the robocalls.³⁴ That number is assigned to HomeyTel, which did not authorize Moser to use its number and which denies any association with these calls.³⁵ Braun, upon receipt of a cease-and-desist letter from the Graham campaign, responded that “[n]either I nor HomeyTel have anything to do with the calls.”³⁶

15. Moreover, Moser had actual knowledge that the phone number he used belonged to HomeyTel. Moser listed HomeyTel’s telephone number on documents he filed in multiple legal actions against HomeyTel.³⁷ Thus, evidence supports the tentative conclusion that Moser apparently knew that he was transmitting misleading or inaccurate caller ID information.

³² *Moser v. Health Insurance Innovations, Inc. et al.*, Case No. 17-CV-1127-WQH-KSC, para. 96 (S.D. CA filed Jun. 5, 2017) (case pending).

³³ Based on the evidence collected during this investigation, the Enforcement Bureau, concurrently with this NAL, is citing Moser for failure to comply with the TCPA’s prerecorded call identification requirements and for making illegal prerecorded voice message calls to wireless numbers without the consumer’s consent. Those violations are separate from, and in addition to, the apparent spoofing violations set forth in this NAL. *Supra* note 3.

³⁴ Dialing Platform Response at Call Detail Records and File Response at 5 (“Once an account is established, users with necessary credentials can access their accounts and create any number of calling campaigns. Mr. Moser did this without [the third party dialing platform’s] involvement, and set the Caller ID.”).

³⁵ Braun Decl.

³⁶ Hiltachk Letter, Exhibit B (E-mail from HomeyTel to Brian T. Hildreth (May 31, 2018, 19:08 PDT)).

³⁷ *E.g.*, 2012 *Moser TCPA* (on file in EB-TCD-18-00028267) (Plaintiff’s Claim and Order to Go to Small Claims Court).

B. Moser Apparently Intended to Cause Harm and Wrongfully Obtain Something of Value

16. The Truth in Caller ID Act prohibits caller ID spoofing with the intent to defraud, cause harm, or wrongfully obtain anything of value. The investigation revealed that Moser apparently met the intent requirement. 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.”³⁸ Courts have recognized that direct evidence of specific intent is rarely available.³⁹ Therefore, it is reasonable and often necessary to look at a party’s actions to determine the party’s intent regarding a wrongful action.⁴⁰ We find from the evidence that Moser apparently intended to cause harm both to HomeyTel and to consumers who received his calls. He also apparently intended to wrongfully obtain something of value by concealing his identity through spoofed caller ID.

1. Moser Apparently Intended to Harm a Specific Business Rival

17. Moser’s robocalls all displayed the same telephone number—one assigned to HomeyTel. The only way to cause HomeyTel’s number to show up in the caller ID for calls that originated from an unrelated company was for someone to select that number and enter it into the robocall platform.⁴¹ Evidence indicates that Moser selected that number deliberately because it would harm HomeyTel and its owner, Braun. Moser, Braun, and HomeyTel have a long, litigious history,⁴² which is reflected in TCPA private right of action lawsuits that Moser brought against Braun and HomeyTel. Moser incontrovertibly knew that the number he used in the caller ID information was HomeyTel’s phone number based on several court filings he has made in his litigation with HomeyTel where the number in question appeared.⁴³

18. The Bureau’s investigation uncovered significant evidence that Moser apparently intended to harm HomeyTel and Braun. By spoofing HomeyTel’s number, Moser caused the victims of the illegal robocalling campaign to misdirect their outrage and complaints at HomeyTel rather than himself. Because the caller ID information showed HomeyTel’s number and the call did not include any

³⁸ *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Report and Order, 26 FCC Rcd 9114, 9122, para. 22 (2011) (*Truth in Caller ID Order*).

³⁹ *United States v. Dearing*, 504 F.3d 897, 901 (9th Cir. 2007); *United States v. Mirabelles*, 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)).

⁴⁰ *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) (“intent to defraud is ordinarily proved by circumstantial evidence”); see also *United States v. Sullivan*, 522 F.3d 967, 974 (9th Cir. 2008) (“the 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 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)).

⁴¹ Dialing Platform Response at Call Detail Records and File Response at 5 (“Once an account is established, users with necessary credentials can access their accounts and create any number of calling campaigns. Mr. Moser did this without [the third party dialing platform’s] involvement, and set the Caller ID.”).

⁴² 2008 Moser TCPA, 2012 Moser TCPA, 2015 Moser TCPA, 2013 Braun.

⁴³ E.g., 2012 Moser TCPA (filed Aug. 29, 2012) (on file in EB-TCD-18-00028267) (Plaintiff’s Claim and Order to Go to Small Claims Court filed by Moser includes HomeyTel phone number of 619-223-1022).

telephone number for consumers to reach the actual initiator of the calls, consumers receiving the thousands of unlawful robocalls directed their complaints to HomeyTel. While the content of calls is not relevant to our determination, Moser's choice to assign his competitor's phone number to these calls demonstrates his intent to harm his competitor. That company received numerous irate calls from consumers, demanding that HomeyTel "stop sending me these disgusting voicemails" and "stop calling my number" and questioning "why are you [autocalling] me with false information."⁴⁴ One particularly enraged consumer misdirected his anger to HomeyTel in a voicemail: "I don't want you calling me back," the consumer said, adding, "*You guys [at HomeyTel] are despicable pieces of sh**.*"⁴⁵ A comparison of these complaints with call records revealed that Moser, not HomeyTel, called complainants.⁴⁶

19. HomeyTel also received a cease and desist letter from candidate Graham. Graham likewise believed that HomeyTel was sending robocalls containing false accusations about him practically on the eve of an election.⁴⁷ That the information was false is irrelevant to our inquiry, but Graham's letter to HomeyTel demonstrates Moser's desire to harm HomeyTel's business.

20. HomeyTel markets itself as a legitimate company offering legal robocalling services to political candidates. By spoofing HomeyTel's phone number to make unlawful robocalls, Moser damaged HomeyTel's reputation and threatened its goodwill to potential customers. Moreover, Moser's own statements about the frustrations of receiving unwanted calls, and the fact that HomeyTel previously complained about an earlier incident in which Moser spoofed HomeyTel's number, support our finding that Moser apparently intended to harm HomeyTel.

2. Moser Apparently Intended to Harm Consumers by Subjecting Them to Illegal Robocalls

21. The TCPA prohibits transmitting prerecorded voice messages to wireless phones unless the called party has given consent, or the call is for an emergency purpose.⁴⁸ Evidence indicates that Moser lacked the requisite consent. Moser made 47,610 robocalls on May 30 and 31, 2018, including calls to more than 11,000 wireless phones, using a prerecorded voice message.⁴⁹ Bureau staff contacted multiple recipients of the robocalls at issue to confirm that: (1) they were the subscribers of the called wireless telephone numbers; (2) they received the calls; and (3) they had not given Moser permission to robocall them. Of the 44 people with whom Bureau staff spoke, none recalled giving Moser, Marketing Support Systems, and/or Jennifer Jones permission to call them on their wireless phones, and nine

⁴⁴ E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 9, 2019, 16:32 EST) (on file in EB-TCD-18-00028267) (voice mail from ██████████ to HomeyTel (May 31, 2018)); E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 7, 2019, 16:33 EST) (on file in EB-TCD-18-00028267) (voice mail from ██████████ to HomeyTel (May 31, 2018)); E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 7, 2019, 17:32 EST) (on file in EB-TCD-18-00028267) (voice mail from ██████████ to HomeyTel (May 30, 2018)). We further note that whether the information is true or false is irrelevant to our inquiry. Moser's actions would still violate the Truth in Caller ID Act had the allegations been true.

⁴⁵ E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 7, 2019, 16:11 EST) (on file in EB-TCD-18-00028267) (voice mail from ██████████ to HomeyTel (May 30, 2018)) (emphasis added).

⁴⁶ Call Detail Records.

⁴⁷ Hiltachk Letter, Exhibit A (Letter from Brian T. Hildreth, Counsel to State Assembly candidate Philip Graham, to HomeyTel Network (May 31, 2018)).

⁴⁸ 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).

⁴⁹ Dialing Platform Response at Call Detail Records; *supra* note 20.

affirmatively stated that they did not.⁵⁰ Thus, the only probative evidence indicates that Moser lacked consent, and the calls did not fall within any other exception to the TCPA. There is no evidence to suggest that Moser had consent for any of the calls to wireless phones.

22. The TCPA requires prerecorded message calls to include the phone number of the entity responsible for initiating the call. Moser did not include this information in the May 2018 calls.⁵¹ Staff listened to the voice file provided by the third party dialing platform, and it failed to mention any phone number.⁵² The only identification information referenced “Jennifer Jones” as the sponsor of the call.⁵³ As a result of Moser’s failing to obtain consent for the calls to wireless phones, and his failing to include the phone number of the initiating caller in the call, the Bureau is issuing a Citation and Order, finding that Moser violated the TCPA. The Commission has found that spoofing, when done in conjunction with an illegal robocalling campaign, can indicate an intent to cause harm.⁵⁴

23. In addition to the fact that the spoofing occurred as part of an unlawful robocalling campaign, there is further reason to conclude that Moser apparently had the requisite intent to harm. *First*, Moser, through Marketing Support Systems, holds himself out as a provider of telemarketing services; the very service that his business offers is governed by the TCPA.⁵⁵ He is thus familiar with the requirements and restrictions of the TCPA.⁵⁶

24. *Second*, Moser himself has filed or participated in more than a dozen complaints alleging TCPA violations in the courts,⁵⁷ including complaints that allege that robocallers sent prerecorded voice messages to his wireless phone number in violation of the TCPA.⁵⁸ Moser’s own statements, made in these court filings prior to the time of Moser’s actions at issue here, show that he understands the provisions of the TCPA and, more particularly, the harm that TCPA violations can inflict. Indeed, in one of his lawsuits, Moser contended that he was harmed in a variety of ways by illegal robocalls, including:

[T]he direct waste of [] time during the call itself, the indirect waste of time in having to break from other important tasks and spend time catching up after the junk call, the waste of telephone

⁵⁰ Declaration of ██████████, dated April 5, 2019 (on file in EB-TCD-18-00028267) and Declaration of ██████████, dated March 27, 2019 (on file in EB-TCD-18-00028267).

⁵¹ Dialing Platform Response at File PHILGRAHAM_REV_VO.MP3 (on file in EB-TCD-18-00028267).

⁵² *Id.*; see also 47 U.S.C. § 227 (d)(3)(A); 47 CFR § 64.1200(b)(2). In response to the subpoena, the third party dialing platform provided the referenced voice file and averred that it was not aware of any other recorded messages or other sound files associated with the calling campaign. Dialing Platform Response at File Response at 5.

⁵³ Bureau staff has been unable to identify a specific person named “Jennifer Jones” associated with Moser or the robocalls in question.

⁵⁴ *Roesel Forfeiture Order*, 33 FCC Rcd at 9218-19, paras. 40-41; *Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6408, para. 16. Indeed, spoofing can further an illegal robocalling campaign. A call recipient is more likely to be induced to answer a call if, for example, the spoofed number appears to be from someone in the community.

⁵⁵ See *Marketing Support Systems BBB Profile*; see also Yellow Pages, Marketing Support Systems Listing, <https://www.yellowpages.com/san-diego-ca/mip/marketing-support-systems-485309814> (Marketing Support Systems appears in the “telemarketing services” section of The Real Yellow Pages) (last visited Nov. 18, 2019).

⁵⁶ 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.”).

⁵⁷ *Supra* notes 27, 28, 29, 31, and 32.

⁵⁸ *Moser v. Health Insurance Innovations, Inc. et al.*, Case No. 17-CV-1127-WQH-KSC (S.D. CA filed Jun. 5, 2017). The allegations of TCPA violations in the Complaint specifically distinguish between calls made to Moser’s wireless phone number and his landline, which shows that Moser possessed knowledge of the TCPA and the different provisions related to each.

service . . . the costs of having to pursue legal remedies, and in the aggravation and consequent health effects of stress these illegal intrusions have caused.⁵⁹

Moser further asserted that he was harmed “by the calls he did not answer [by] . . . having to check the Caller ID while he was busy in meetings”⁶⁰ Indeed, Moser admitted that he relies on caller ID information to determine whether to answer a call and that receiving illegal robocalls can cause significant harm, including aggravation and stress.

25. In light of Moser’s acknowledgement of the significant harm that unlawful robocalls impose, we find it reasonable to conclude that he intended to inflict that harm on others. Moser’s experience presumably made him well aware that spoofing another company’s number, without providing a call back number in the call, would make it impossible for consumers receiving his robocalls to return the calls to request not to be called again. Thus, we find that Moser apparently intended to harm consumers through the use of spoofed calls in furtherance of his illegal robocalling campaign.

3. Moser Apparently Intended to Wrongfully Obtain a Valuable Shield Against Culpability and Lawsuits

26. Evading detection and prosecution for unlawful acts has significant value. Courts have held that “anything of value” is not limited to tangible assets.⁶¹ The Commission has recognized that “avoidance of culpability is a benefit that qualifies as a thing of value.”⁶² In this case, Moser’s attempt to avoid law enforcement (and thereby culpability for these calls) by spoofing the caller ID in order to make calls for which he was paid has an ascertainable dollar value. Specifically, the Commission has authority to impose a penalty of up to \$20,134 for each robocall made in violation of the TCPA rules,⁶³ and a recipient of such calls may bring a private right of action for violation of the TCPA and receive at least \$500 for each such violation. If the court finds that the defendant in such private right of action willfully or knowingly violated the TCPA or its implementing rules, the court may award up to \$1,500, treble damages, to the plaintiff for each violation.⁶⁴

⁵⁹ *Id.* at para. 96.

⁶⁰ *Id.* at para. 97.

⁶¹ *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. 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.”); see *United States v. Picquet*, 963 F.2d 54, 55 (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 (7th Cir. 1997) (agreeing with and applying 5th Circuit’s expansive interpretation of phrase “anything of value” in *Picquet*); *United States v. Schwartz*, 785 F.2d 673, 680 (9th Cir. 1986) (noting 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).

⁶² *Roesel Forfeiture Order*, 33 FCC Rcd at 9212, para. 22; *Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6413, para. 27.

⁶³ *Amendment of Section 1.80(b) of the Commission’s Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, 33 FCC Rcd 12278, 12283 (EB 2018) (*2019 Inflation Order*).

⁶⁴ 47 U.S.C. § 227(b)(3).

27. Moser is aware of the potential cost of private TCPA lawsuits, as he has brought such cases multiple times.⁶⁵ Thus, it is reasonable to infer that Moser intended to shield himself from liability and culpability for violation of the TCPA. In addition, Moser's telemarketing business includes robocalling, and he was paid for making these calls. Therefore, we find that Moser apparently knowingly spoofed the HomeyTel phone number to wrongfully obtain something of value.

28. We find that during the two-day calling campaign, Moser made 47,610 apparently unlawful spoofed calls. We conclude that each call was spoofed using HomeyTel's caller ID information, and that Moser made 47,610 spoofed robocalls with the apparent intent to cause harm and wrongfully obtain something of value—each call an apparent violation of the Truth in Caller ID Act and our rules.

C. Proposed Forfeiture

29. Section 227(e) of the Act, which empowers the FCC “to proceed expeditiously . . . without first issuing a citation,”⁶⁶ and section 1.80 of the Commission's rules authorize us to impose a forfeiture against any person that engages in unlawful spoofing.⁶⁷ Specifically, the Act and the Commission's rules authorize a forfeiture of up to \$11,562 for each spoofing violation, or three times that amount for each day of a continuing violation, up to a statutory maximum of \$1,156,242 for any single act or failure to act.⁶⁸ 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.”⁶⁹ 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.⁷⁰ Under

⁶⁵ As noted, in addition to the TCPA litigation with HomeyTel and legions of other TCPA cases filed in small claims court in California, Moser has also sued several other companies in federal district court alleging TCPA violations. *Supra* notes 31 and 32.

⁶⁶ *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) 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.

⁶⁷ 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 Moser apparently willfully and repeatedly spoofed caller ID information with the intent to harm and to wrongfully obtain something of value.

⁶⁸ 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).

⁶⁹ 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.

⁷⁰ 47 CFR § 1.80(b)(8), Note to paragraph (b)(8).

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.⁷¹

30. The Commission has proposed a base forfeiture of \$1,000 per unlawful spoofed call in past mass-spoofing enforcement actions. We came to the \$1,000 figure because we determined 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.⁷² We have discretion, however, to propose a higher amount up to the statutory maximum of \$11,562, and a strong congressional directive to take action necessary to pursue and punish perpetrators of unlawful spoofing. We thus propose a base forfeiture amount of \$1,000 per violation.

31. As with past Commission actions addressing violations of section 227(e), we do not apply the base forfeiture to all 47,610 apparently unlawful spoofed calls; rather, we apply the base forfeiture to a subset of the apparently unlawful spoofed calls 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 resulted in a proposed forfeiture that was sufficient to achieve the dual goals of penalizing wrongful conduct and preventing it from recurring.⁷³ Each case is unique, and we must use our discretion in proposing an appropriate penalty to meet the specific circumstances.⁷⁴ In this case, Bureau staff analyzed 5,713 apparently unlawful spoofed calls.⁷⁵ Applying the base forfeiture to these analyzed violations yields a total base forfeiture of \$5,713,000.

32. In weighing the harm Moser caused to HomeyTel and call recipients, and the scale and scope of the unlawful spoofing campaign, we find that, in applying the statutory factors in section 503 of the Act and section 1.80 of the Commission's rules,⁷⁶ the totality of the circumstances in this case merit a significant upward adjustment to the base penalty.

33. Most unlawful spoofing campaigns use spoofed caller ID information to evade angry call-backs and deter law enforcement action,⁷⁷ or to encourage consumers to answer the phone by selecting caller ID information that appears to be coming from a neighbor,⁷⁸ or a trusted source.⁷⁹ Moser,

⁷¹ *Id.*

⁷² In unlawful spoofing campaigns of millions of calls, a higher per-violation amount would quickly reach astronomical levels. For example, if we were to assess a base forfeiture amount close to the statutory maximum, e.g., \$10,000 for each of say, 75 million unlawful spoofed calls, the forfeiture would be \$750,000,000,000, *i.e.*, three quarters of a trillion dollars.

⁷³ *Affordable Enterprises of Arizona, LLC*, Notice of Apparent Liability for Forfeiture, 33 FCC Rcd 9233, 9245-46, paras. 34-35 (2018); *Roesel Forfeiture Order*, 33 FCC Rcd at 9225, paras. 57-58; *Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6414, paras. 32-33.

⁷⁴ See *RKO General, Inc.*, 670 F.2d at 237, citing *Leflore Broadcasting Co.*, 636 F.2d at 463 (“We have made it clear in earlier cases that ‘the choice of remedies and sanctions is a matter wherein the Commission has broad discretion.’”).

⁷⁵ Reviewed Call Detail Records (on file EB-TCD-18-00028267) (containing the call records Bureau staff selected for analysis, including the date and times the call were made).

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

⁷⁷ *E.g.*, *Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6413, para. 27.

⁷⁸ *E.g.*, *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, Notice of Apparent Liability for Forfeiture, 32 FCC Rcd 5418, 5422-23, paras. 17-18 (2017) (*Abramovich NAL*).

⁷⁹ *E.g.*, *IRS, Don't Be Fooled, Phone Scams Continue to Be Serious Threat Nationwide*, IR-2015-62, (Mar. 31, 2015), <https://www.irs.gov/newsroom/dont-be-fooled-phone-scams-continue-to-be-serious-threat-nationwide> (IRS

however, apparently deliberately selected the caller ID information specifically to damage the reputation of HomeyTel, a company with which he had extensive, negative dealings. His intent to harm with this spoofing campaign rises to a level beyond that which the Commission has typically seen before in unlawful spoofing cases. Beyond the harm caused to call recipients, which is similar to what we have seen in past enforcement actions,⁸⁰ Moser intentionally targeted one company when he set the caller ID information to show HomeyTel's phone number in each of the more than 47,000 apparently unlawful spoofed calls. In doing so, Moser's calls threatened the reputation and goodwill of HomeyTel, and exposed the company to significant risk of private litigation under the TCPA.

34. Bureau staff also discovered evidence that Moser's May 2018 conduct was not isolated. Moser previously conducted a robocalling campaign, on November 3 and 5, 2016, and set the caller ID information to show HomeyTel's telephone number.⁸¹ Similar to the facts in the May 2018 unlawful spoofed calling campaign, Moser was not authorized to use HomeyTel's phone number,⁸² had ongoing litigation with HomeyTel and Braun,⁸³ and caused HomeyTel to receive a number of complaints from consumers even though HomeyTel had not placed the calls.⁸⁴

35. While the forfeiture we propose here is based solely on the unlawful spoofed calls made on May 30 and 31, 2018, we may consider other past conduct in determining an adjustment to a base forfeiture amount.⁸⁵ We find that, based on Moser's pattern of conduct, Moser is highly culpable and his behavior is egregious. We therefore propose a 75% upward adjustment to the base penalty yielding a total forfeiture amount of \$9,997,750.

36. Additionally, we hold Kenneth Moser personally liable for the consequences of his apparently unlawful actions. Bureau staff found no evidence that Marketing Support Systems is a legally incorporated entity.⁸⁶ Rather, Kenneth Moser operates Marketing Support Systems in his individual

warning taxpayers not to be fooled by phone scammers who "alter caller ID numbers to make it look like the IRS is calling").

⁸⁰ *E.g., Roesel Forfeiture Order*, 33 FCC Rcd at 9218-19, paras. 40-41; *Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6408, para. 16.

⁸¹ Second Dialing Platform Response. [REDACTED] confirmed that Moser was the contact listed for that account in November 2016. *Id.*

⁸² *Supra* para. 9.

⁸³ *Supra* para. 10.

⁸⁴ *Supra* para. 9. E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 7, 2019, 14:44 EST) (on file in EB-TCD-18-00028267) (voice mail from [REDACTED] to HomeyTel (Nov. 5, 2016)); E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 7, 2019, 15:46 EST) (on file in EB-TCD-18-00028267) (voice mail from [REDACTED] to HomeyTel (Nov. 3, 2016)); E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 7, 2019, 14:47 EST) (on file in EB-TCD-18-00028267) (voice mail from [REDACTED] to HomeyTel (Nov. 3, 2016)). A comparison of these complaints with call records revealed that Moser, not HomeyTel, called complainants. Second Dialing Platform Response.

⁸⁵ *AT&T Inc., Parent Company of New Cingular Wireless PCS, LLC and AT&T Mobility Puerto Rico, Inc.*, Notice of Apparent Liability for Forfeiture 30 FCC Rcd 856, 859, n.26, 861, para. 12 and 862, n.42 (2015) (Commission stating that "Section 503 of the Act does not bar the Commission from assessing whether AT&T's conduct prior to [the applicable statute of limitations period] apparently violated the Act or Rules or considering such conduct in determining the appropriate forfeiture amount for violations that occurred within the [statute of limitations period]."); *Order*, 31 FCC Rcd 10484 (EB 2016) (adopting Consent Decree); *see also Enserch Corp.*, Forfeiture Order, 15 FCC Rcd 13551, 13554, para. 11 (2000).

⁸⁶ In addition to Bureau staff's discovery that Moser registered Marketing Support Systems as a fictitious business name, Bureau staff reviewed the California Secretary of State website, which provides information on corporations,

capacity under a fictitious business name.⁸⁷ As such, he is not entitled to the protection of the corporate form and is personally liable for the apparent violations.⁸⁸ Accordingly, we hold Moser dba Marketing Support Systems liable for the proposed forfeiture.

IV. ORDERING CLAUSES

37. **IT IS ORDERED** that, pursuant to sections 227(e)(5)(A)(i) and 503(b) of the Act⁸⁹ and sections 1.80 of the Commission's rules,⁹⁰ Kenneth Moser dba Marketing Support Systems is hereby **NOTIFIED** of this **APPARENT LIABILITY FOR A FORFEITURE** in the amount of nine million, nine hundred ninety-seven thousand, seven hundred fifty dollars (\$9,997,750) for willful and repeated violations of section 227(e) of the Act,⁹¹ section 64.1604 of the Commission's rules,⁹² and the *Rules and Regulations Implementing the Truth In Caller ID Act of 2009*.⁹³

38. **IT IS FURTHER ORDERED** that, pursuant to section 1.80 of the Commission's rules,⁹⁴ within thirty (30) calendar days of the release date of this Notice of Apparent Liability for Forfeiture, Kenneth Moser dba Marketing Support Systems, **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 41-42 below.⁹⁵

39. 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. Kenneth Moser dba Marketing Support Systems shall send electronic notification of 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.⁹⁶ When completing the FCC Form 159, enter the Account Number in block number 23A (call sign/other ID) and enter the letters "FORF" in

limited liability corporations, and limited partnerships incorporated in the state, and found no evidence that Marketing Support Systems is currently operating or has operated under corporate or partnership structure in California. California Secretary of State, *Business Search*, <https://businesssearch.sos.ca.gov> (visited Aug. 23, 2018).

⁸⁷ *Supra* notes 2 and 16.

⁸⁸ See *Labadie Coal Co. v. Black*, 672 F.2d 92, 95 (D.C. Cir. 1982) (noting that piercing the corporate veil analysis to find personal liability is only relevant "if it is established that the corporate entity itself exists"); *Abramovich NAL*, 32 FCC Rcd at 5427-28, para. 27; see also *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, Forfeiture Order, 33 FCC Rcd 4663, 4674, para. 33 ("[B]ecause Mr. Abramovich continued to operate under the name of a dissolved corporation, Marketing Strategy Leaders, during the time the violations occurred, he is not entitled to the protections of the corporate form and is personally liable for the full forfeiture amount.") (*Abramovich Forfeiture Order*).

⁸⁹ 47 U.S.C. §§ 227(e)(5)(A)(i) and 503(b).

⁹⁰ 47 CFR § 1.80.

⁹¹ 47 U.S.C. § 227(e).

⁹² 47 CFR § 64.1604.

⁹³ *Truth in Caller ID Order*.

⁹⁴ 47 CFR § 1.80.

⁹⁵ 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.

⁹⁶ An FCC Form 159 and detailed instructions for completing the form may be obtained at <http://www.fcc.gov/Forms/Form159/159.pdf>.

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.

40. 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 20554.⁹⁷ 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.

41. 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.⁹⁸ 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 Sonja Rifken, Attorney, Telecommunications Consumers Division, at Sonja.Rifken@fcc.gov.

42. 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; and (3) any other reliable and objective documentation that accurately reflects the petitioner's current financial status.⁹⁹ Any claim of inability to pay must specifically identify the basis for the claim by reference to the financial documentation.

⁹⁷ See 47 CFR § 1.1914.

⁹⁸ *Id.* at §§ 1.16, 1.80(f)(3).

⁹⁹ See *Abramovich Forfeiture Order*, 33 FCC Red at 4678-78, paras. 44-45. We note that such information should also include any judgments or settlements Moser received related to any TCPA litigation in which he was involved.

43. **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 Kenneth Moser dba Marketing Support Systems at [REDACTED].

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

**STATEMENT OF
CHAIRMAN AJIT PAI**

Re: *Kenneth Moser dba Marketing Support Systems, EB-TCD-18-00028267*

One week before last year's California primary election, residents of the 76th State Assembly District outside of San Diego received a robocall describing in graphic terms a sexual assault allegedly committed by one of the candidates running for an open Assembly seat. But the allegation was false. It had already been disproven by law enforcement. It was a malicious smear.

The FCC doesn't (and shouldn't) have the authority to police truthfulness in political campaigns. But we can police unlawfully spoofed robocalls. And that's relevant here because Kenneth Moser, through his telemarketing company, Marketing Support Systems, apparently made 47,000 of these robocalls over the course of two days. When he did that, he didn't include accurate caller ID information. He didn't want people to know that he was making these calls.

Why? The facts strongly suggest that Moser spoofed the caller ID information of a business rival with the intent to harm that rival. He wasn't simply trying to disassociate himself from the calls. If that was the case, he could have inserted random caller ID information. Instead, Moser chose to associate his business rival with these upsetting and false robocalls, which obviously would not be good for the rival's reputation. And indeed, that company bore the brunt of complaints from angry Californians who received these robocalls.

Today, we propose a forfeiture of \$9,997,750 on Moser for these apparently unlawful spoofed robocalls. This Notice of Apparent Liability is the latest, but certainly not the last, of our enforcement efforts to aggressively combat illegal robocalls and protect American consumers. Today's action is a great example of FCC staff's persistence to track down and bring illegal robocallers to justice.

And we are not alone. Thanks to the leadership of Senators John Thune and Ed Markey, and Representatives Frank Pallone and Greg Walden, it looks like additional help is on the way. Their new bill, which has already passed the House, would make a number of reforms. One of them would extend the statute of limitations, which would make it easier for our dedicated Enforcement Bureau staff to bring illegal robocallers to justice.

We are also working with our international partners to combat spoofed robocalls. Just this week, I held the first official cross-border call using the SHAKEN/STIR caller ID authentication framework with Ian Scott, Chairperson and CEO of the Canadian Radiotelevision and Telecommunications Commission. The implementation of SHAKEN/STIR will be a critical step to protect consumers from spoofed robocalls, and we will continue to work domestically and internationally on this important issue. Speaking of which, the end-of-the-year deadline for major carriers to implement SHAKEN/STIR is coming up. I've already directed staff to review the record and draft options for mandating the implementation of SHAKEN/STIR by rule. And if industry does not get the job done, I will not hesitate to call an FCC vote on new rules.

I want to thank Parul Desai, Lisa Gelb, Rosemary Harold, Shannon Lipp, Sonja Rifken, Kristi Thompson, and Shana Yates of the Enforcement Bureau; and Valerie Hill, Richard Mallen, and Bill Richardson of the Office of General Counsel for their tireless efforts to rein in the scourge of illegal robocalls and to protect all Americans.

STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL

Re: *Kenneth Moser dba Marketing Support Systems*, File No.: EB-TCD-00028267, Notice of Apparent Liability for Forfeiture (December 12, 2019)

The phone rings. On the line is someone offering a fabulous cruise or a once-in-a-lifetime investment opportunity. Or maybe it's an agent from the Internal Revenue Service with the threatening news of an imminent lawsuit. They're robocalls. And they are totally out of control.

At the start of this Administration, consumers received roughly 2 billion robocalls a month. They now average between 5 and 6 billion a month. This is crazy. Whatever we are doing to stem the tide of these calls is simply not working. Those numbers show with perfect clarity we need to do more.

It is against this background that today the Federal Communications Commission seeks to enforce its rules and help stop the deluge of robocalls. In the instant decision, we have a particularly ugly set of facts. Kenneth Moser was a telemarketer who launched an extensive robocalling campaign. It spoofed the number of his business rival and sent out calls featuring allegations of sexual assault involving a political candidate.

In response, we propose a \$9.99 million fine to penalize him for this robocalling because it violates the law. This is good because enforcement of our rules designed to prevent robocalls matters.

But it is not enough. Because everyone should save the accolades for when we crush these calls *and collect*. And on that score, we have work to do. Earlier this year, *The Wall Street Journal* found that of the over \$208 million in fines this agency had assessed on those responsible for robocalls, it had collected—wait for it—just \$6,790. That's embarrassing.

In fact, it has gotten so bad that Congress has stepped in with legislative efforts to improve coordination across the government and make it possible for this agency to collect on its enforcement fines. We need it. Because without it our action today is not especially meaningful and—let's be honest—will not stop these nuisance calls from continuing to grow.

**STATEMENT OF
COMMISSIONER GEOFFREY STARKS**

Re: *In the Matter of Kenneth Moser d/b/a Marketing Support Systems*

I am pleased that we are imposing a stiff penalty in this case. Mr. Moser's actions harmed both the company whose number he spoofed and the thousands of people who received his distressing and factually baseless messages. I appreciate the work of the bureau staff in making sure that this conduct is punished, consistent with our responsibilities under the Truth in Caller ID Act.

The facts of this particular case are egregious, but they are not unfamiliar to the millions of Americans who receive unwanted robocalls every day. Unwanted robocalls are a huge and growing problem, and we seem to reach a new record each year. Over the course of this meeting alone, Americans will receive more than 20 million robocalls. This scourge has changed the fabric of our culture – if you're like me and you get a call from a number that you don't recognize, you don't pick it up. And numbers from spoofed calls, which look like they are coming from a local business or neighbor, are especially pernicious because we can't differentiate these unwanted robocalls from calls from our doctors or our kids' schools.

We need a multi-pronged approach to rebuilding trust in our phone system, and vigorous enforcement must be part of our plan. That's why I have been so supportive of the Pallone-Thune TRACED Act. Among other improvements, the TRACED Act will provide new tools, including extending our statute of limitations, that will enhance the Commission's abilities to track down illegal robocallers, stop them, and hold them accountable. I am hopeful that the TRACED Act will be signed into law soon and the Commission will be able to put those tools to work to deter bad actors.