

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

FORFEITURE ORDER

Adopted: November 18, 2020

Released: November 19, 2020

By the Commission: Chairman Pai issuing a statement, Commissioner O’Rielly approving in part,
dissenting in part and issuing a statement, Commissioner Rosenworcel issuing a statement.

TABLE OF CONTENTS

Heading Paragraph #
I. INTRODUCTION..... 1
II. BACKGROUND..... 3
III. DISCUSSION 10
A. Moser Knowingly Engaged in Spoofing..... 11
B. Moser Made Thousands of Spoofed Robocalls with the Intent to Cause Harm and
Wrongfully Obtain Something of Value..... 14
1. Moser Intended to Harm the Spoofed Number’s Subscriber, HomeyTel 16
2. Moser Intended to Harm the Recipients of His Spoofed Robocalls..... 20
3. Moser Falsified Caller ID Information with the Intent to Wrongfully Obtain
Something of Value..... 29
C. All Robocalls are Subject to the Requirements of the TCPA 35
D. The Commission’s Forfeiture is Based Solely on Moser’s Illegal Spoofing, Not the
Content of the Political Message 37
E. The Full Amount of the Forfeiture is Warranted 39
1. The Commission’s Evidence Supports the Forfeiture..... 40
2. The Commission Satisfied Moser’s Fifth Amendment Due Process Rights..... 42
IV. ORDERING CLAUSES..... 48

I. INTRODUCTION

1. Combatting unlawful, unwanted telephone calls—including unlawfully “spoofed”
robocalls—is the Federal Communications Commission’s top consumer protection priority. Spoofing
occurs 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 of 2009 when it is done with
the intent to “defraud, cause harm, or wrongfully obtain anything of value.”¹

¹ 47 U.S.C. § 227(e); 47 CFR § 64.1604 (“No person or entity in the United States . . . shall, with the intent to
defraud, cause harm, or wrongfully obtain anything of value, knowingly cause, directly, or indirectly, any caller
identification service to transmit or display misleading or inaccurate caller identification information[.]”).

2. Today, we affirm our Notice of Apparent Liability (*Notice*)² and find that Kenneth Moser (Moser), doing business as Marketing Support Systems, violated section 227(e) of the Communications Act of 1934, as amended (Communications Act or Act),³ and section 64.1604 of the Commission's rules.⁴ Moser admitted to intentionally spoofing a phone number assigned to HomeyTel Network (HomeyTel), a long-time business rival.⁵ Moser used HomeyTel's number to transmit 47,610 unlawful prerecorded voice calls (i.e., robocalls) to communicate accusations regarding a candidate for an open California State Assembly seat, Mr. Philip Graham (Graham). Moser placed the calls on behalf of an unnamed client who was a relative of one of Graham's fellow candidates.⁶ Moser was not authorized to use HomeyTel's phone number. Moser has a long and contentious relationship with HomeyTel and that company's founder and current manager, Conrad Braun (Braun). As a result of the spoofed robocalls, Braun and HomeyTel received a multitude of complaints from call recipients as well as a cease-and-desist letter from Graham that threatened "imminent litigation."⁷ After reviewing Moser's response to the *Notice*, we find no reason to rescind the *Notice* nor reduce the proposed penalty. Therefore, we affirm the \$9,997,750 forfeiture proposed in the *Notice*.

II. BACKGROUND

3. *Legal Background.* Congress has 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. The Commission has noted that "[c]aller ID allows consumers to screen out unwanted calls and to identify companies that they wish to ask not to call again."⁸ The Commission has further stated that "[k]nowing the identity of the caller is also helpful to consumers who feel frightened or threatened by hang-up and 'dead air' calls."⁹ Caller ID is only valuable, however, if it is accurate.¹⁰ Therefore, Congress passed the Truth in Caller ID Act of 2009 (Truth in Caller ID Act), as codified in section 227(e) of the Act.¹¹ 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

² *Kenneth Moser dba Marketing Support Systems*, Notice of Apparent Liability for Forfeiture, 34 FCC Rcd 12753 (2019) (*Notice*). The *Notice* includes a more complete discussion of the facts and history of this case and is incorporated herein by reference.

³ 47 U.S.C. § 227(e).

⁴ 47 CFR § 64.1604.

⁵ See *Kenneth Moser dba Marketing Support Systems*, Response to Notice of Apparent Liability for Forfeiture, at 5-6 (June 15, 2020) (on file in EB-TCD-18-00028267) (Notice Response).

⁶ *Id.* at 4.

⁷ Letter from Thomas W. Hiltachk, Counsel to State Assembly candidate Philip Graham, to Alex Padilla, California Secretary of State at Exhibit B (June 1, 2018) (on file in EB-TCD-18-00028267) (Hiltachk Letter) (providing an e-mail correspondence between HomeyTel and Brian T. Hildreth).

⁸ *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 18 FCC Rcd 14014, 14121, para. 179 (2003) (*TCPA Order*).

⁹ *Id.*

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

¹¹ 47 U.S.C. § 227(e).

transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value[.]”¹²

4. Congress has also provided significant protections for consumers from unlawful robocalls through the Telephone Consumer Protection Act (TCPA).¹³ The statute and the Commission’s implementing rules prohibit any artificial or prerecorded voice message calls to wireless telephone numbers without the subscribers’ prior express consent unless the calls are made for an emergency purpose.¹⁴ In addition, calls employing artificial or prerecorded voice messages—whether placed to wireless or wireline phones—must identify the entity responsible for initiating the prerecorded voice message call at the beginning of the message and provide a phone number for that entity during or after the message.¹⁵ The Commission has found that spoofing, when done in conjunction with TCPA violations, may indicate an intent to cause harm under the Truth in Caller ID Act.¹⁶

5. *Factual Background.* In 2018, the Commission learned that Moser had engaged in a large-scale robocalling campaign in which he intentionally caused a caller identification service to display falsified caller ID information to call recipients in California.¹⁷ Based upon a complaint referred by the California Secretary of State,¹⁸ the Commission’s Enforcement Bureau (Bureau) initiated an investigation. Bureau staff traced the robocalls to a third-party dialing platform, {{ }}, which disclosed that Moser and Marketing Support Systems made 47,610 robocalls in a two-day robocalling campaign, including repeated calls to the same recipients.¹⁹ The investigation uncovered that Moser intentionally set the caller ID information for all of the 47,610 calls he made to display one phone number, 619-223-1022,²⁰ which belonged to HomeyTel, a company formerly owned and currently managed by Braun.²¹ Moser is not affiliated with HomeyTel and was not authorized to use its phone

¹² *Id.*; see also 47 CFR § 64.1604. There are exceptions for investigative, protective, or intelligence activities, but those exceptions do not apply here.

¹³ 47 U.S.C. §§ 227(b), (d)(3).

¹⁴ *Id.* § 227(b)(1)(A)(iii); 47 CFR § 64.1200(a)(1)(iii).

¹⁵ 47 U.S.C. § 227(d)(3)(A); 47 CFR § 64.1200(b)(1)-(2). Although this *Order* imposes a forfeiture for violations of the Truth in Caller ID Act, the TCPA is relevant to our determination that Moser acted to wrongfully obtain something of value (one element of the Truth in Caller ID Act) because he violated the TCPA.

¹⁶ *Best Insurance Contracts, Inc., and Philip Roesel, dba Wilmington Insurance Quotes*, Forfeiture Order, 33 FCC Rcd at 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*); *Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, Notice of Apparent Liability, 32 FCC Rcd 5418, 5423, para. 16 (2017).

¹⁷ E-mail from {{ }} 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 {{ }} to Sonja Rifken, Attorney Advisor, 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). Material set off by double brackets {{ }} is confidential and is redacted from the public version of this document.

¹⁸ Letter from Steven J. Reyes, Chief Counsel to California Secretary of State, to Rosemary Harold, Chief, FCC Enforcement Bureau et al. (June 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. See Hiltachk Letter.

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

²⁰ See Dialing Platform Response at Call Detail Records and File Response at 5.

²¹ See E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney Advisor, 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

number.²² Moser admits that he intentionally selected and transmitted that spoofed telephone number for his calling campaign and that he knowingly used a number that was not affiliated with his own business.²³ Moser also admits that he intentionally selected the number knowing that it had been affiliated with HomeyTel.²⁴

6. 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 prerecorded voice message that graphically described an alleged sexual assault involving Graham, one of eight candidates for an open State Assembly seat.²⁵ More than 11,000 of the 47,610 robocalls were sent to wireless phones.²⁶ The record shows that the calls to wireless numbers were made without the called parties' consent.²⁷ None of the 47,610 prerecorded voice messages included the telephone number of the party responsible for initiating the call or any other identifying information. The prerecorded message stated only that it was "paid for by Jennifer Jones," which Moser admits is a pseudonym.²⁸ In reality, Moser made the calls on behalf of a client who was a relative of a candidate opposing Graham for the State Assembly seat.²⁹

7. Moser was familiar with the TCPA and other relevant law. Indeed, he has found himself on both sides of complaints alleging TCPA violations. More specifically, he has filed or participated in at least 15 complaints alleging TCPA violations by various companies,³⁰ including multiple complaints

Chief, Telecommunications Consumer Division, FCC Enforcement Bureau, to {
}] (Mar. 4, 2019) (on file in EB-TCD-18-00028267); E-mail from {
}], to Jermaine Haynes, Senior Analyst, Telecommunications Consumer Division, FCC Enforcement Bureau (Mar. 5, 2019, 9:28 EST) (on file in EB-TCD-18-00028267) (BNA Response) (confirming that HomeyTel is subscriber).

²² Braun Decl.

²³ Notice Response at 5-6.

²⁴ *Id.*

²⁵ See Jesse Marx, *Telemarketer Says Another GOP Campaign Was Behind Phil Graham Robocalls*, Voice of San Diego (July 10, 2020), <https://www.voiceofsandiego.org/topics/politics/telemarketer-says-another-gop-campaign-was-behind-phil-graham-robocalls/>; 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/>.

²⁶ 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 Oct. 8, 2020).

²⁷ 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 said that they gave Moser, Marketing Support Systems, and/or Jennifer Jones permission to call them on their wireless phones, and none of the call recipients stated that they provided express consent. Declaration of {
}] (filed Apr. 5, 2019) (on file in EB-TCD-18-00028267); Declaration of {
}] (filed Mar. 27, 2019) (on file in EB-TCD-18-00028267).

²⁸ Dialing Platform Response at File PHILGRAHAM_REV_VO.MP3 (on file in EB-TCD-18-00028267).

²⁹ Notice Response at 4 ("MSS was referred and introduced to a new client who wanted to do an independent expenditure political calling campaign in support of a relative competing on the ballot along with Philip Graham."). Moser clarifies that the client was a relative of Maureen and Mark Muir. See *id.* at 4, Exhibit K. Moser also states on multiple occasions that he intentionally did not disclose his client's true identity. *Id.* at 5-7.

³⁰ See, 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 July 12, 2017); *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 (filed

against HomeyTel and Braun.³¹ When Moser has been the complainant or plaintiff, he has asserted that TCPA violations cause harm, including harm from the “aggravation and consequent health effects of stress these illegal intrusions have caused.”³² Moser has also been accused of committing TCPA violations, including a prior instance in 2016 in which Moser spoofed HomeyTel’s caller ID information to conduct a robocalling campaign without first obtaining HomeyTel’s consent.³³

8. On December 13, 2019, the Commission released the *Notice* proposing a \$9,997,750 forfeiture against Kenneth Moser for his apparent willful and repeated violations of section 227(e) of the Act³⁴ and section 64.1604 of the Commission’s rules³⁵ by spoofing caller ID information with the intent to cause harm and wrongfully obtain something of value.³⁶

9. On June 15, 2020, Moser submitted a response to the *Notice*, arguing that the *Notice* should be rescinded.³⁷ Moser argues that the political content of the spoofed calls exempts him from any liability under the TCPA and the Commission’s rules.³⁸ Moser admits that he intentionally made spoofed

Oct. 23, 2015); *Engle, Moser v. Unified Life Insurance Co., Inc., et al*, Case No. 14-CV-1908-MMA-JLB (S.D. CA filed Aug. 13, 2014).

³¹ 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 seven years in small claims court in San Diego County. In one case, he alleged that Braun and/or HomeyTel violated the TCPA by making “illegal automated phone message [calls] soliciting toner products.” *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). In a second case, Moser claimed that HomeyTel violated the Truth in Caller ID Act and the TCPA by making “illegal auto dial advertising [calls].” *Moser v. HomeyTel et al.*, Case No. 37-2012-00005170-SC-SC-CTL (filed Aug. 29, 2012). And in a third case, Moser alleged that Braun violated the Truth in Caller ID Act and made “illegal robo call[s].” *Moser v. Braun*, Case No. 37-2015-00322367-SC-SC-CTL (filed June 8, 2015) (alleging fraud, breach of settlement, and TCPA violations).

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

³³ During the course of the investigation, Commission staff subpoenaed {{ }}, and in reviewing the subpoena response, we uncovered a prior robocalling campaign in which Moser spoofed HomeyTel’s phone number in 2016. Letter from Kristi Thompson, Division Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to {{ }} (Mar. 22, 2019) (on file in EB-TCD-18-00028267) (subpoenaing call detail records and certain contact information). {{ }} provided the subpoenaed information to the Bureau on March 25, 2019. E-mail from {{ }} to Parul Desai, Deputy Chief, Telecommunications Consumers Division, FCC Enforcement Bureau (Mar. 25, 2019, 16:17 EDT) (on file in EB-TCD-18-00028267) (Second Dialing Platform Response). {{ }} confirmed that Moser was the contact listed for that account in November 2016. *Id.*; see also E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (Mar. 28, 2019, 22:21 EDT) (on file in EB-TCD-18-00028267) (Braun Supplemental Decl.) (stating that neither Moser nor Marketing Support Systems was authorized to use the HomeyTel number in November 2016).

³⁴ 47 U.S.C. § 227(e).

³⁵ 47 CFR § 64.1604.

³⁶ 47 U.S.C. § 227(e).

³⁷ Notice Response.

³⁸ *Id.* at 1-2, 6-10, 13. For example, Moser argues that “the FCC completely overstretched its legal mandate and ignored both the 1st [A]mendment protections on political speech for the Order and Notice in addition to the 5th [A]mendment requirements for due process in issuing the Notice,” and “MSS only does non-profit or not for profit political messages which are protected 1st Amendment speech and exempt from the TCPA per §227(a)(4),” and “[I] didn’t think anyone would bother [to trace back] an exempt political message.” *Id.* at 2, 10, 15.

telephone calls, but argues that he was unaware that the number still belonged to HomeyTel.³⁹ Moser asserts that Braun no longer lived or operated in the United States⁴⁰ and, when he called HomeyTel's 619-223-1022 phone number, it went directly to a voicemail answering machine.⁴¹ Therefore, Moser claims he believed HomeyTel's telephone number was no longer in service and, consequently, that he did not intend to cause harm to HomeyTel.⁴² He likewise states that he did not intend to harm consumers.⁴³ Moser further claims that the call recipients all consented to receive robocalls for political purposes when they registered to vote.⁴⁴ Moser also asserts that he did not intend to "wrongfully obtain anything of value"⁴⁵ and that the Commission's definition of "anything of value" is not supported by the case law.⁴⁶ However, he contends that even if the Commission correctly defined "anything of value," his only intent in spoofing was to protect his client's identity.⁴⁷ Finally, Moser argues that the Commission did not afford him his due process rights⁴⁸ and alleges that the Commission's *Notice* is the result of a "politically motivated investigation."⁴⁹

III. DISCUSSION

10. The Commission proposed a forfeiture in accordance with section 503(b) of the Act,⁵⁰ section 1.80 of the Commission's rules,⁵¹ and the Commission's *Forfeiture Policy Statement*.⁵² We have fully considered Moser's response to the *Notice*, which includes a variety of legal and factual arguments, but we deem none of them persuasive. We therefore affirm the \$9,997,750 forfeiture proposed in the *Notice*.

A. Moser Knowingly Engaged in Spoofing

11. We find that Moser violated section 227(e) of the Act and section 64.1604 of the Commission's rules by knowingly transmitting or displaying inaccurate caller ID information.⁵³ The evidence in the record, including Moser's own admissions, squarely establishes that Moser falsified caller ID information by selecting and displaying a number that he had no right to use.⁵⁴ That number was

³⁹ *Id.* at 11.

⁴⁰ *Id.* at 4.

⁴¹ *Id.* at 11.

⁴² *Id.* at 1-3, 5-6, 8, 11, 13.

⁴³ *Id.* at 2, 5, 12-13.

⁴⁴ *Id.* at 5.

⁴⁵ *Id.* at 5-6, 12-13.

⁴⁶ *Id.* at 12.

⁴⁷ *Id.* at 2 ("We [spoofed the caller ID] at the request of our client so as to protect her identity as she wanted to remain anonymous . . ."); *id.* at 5 ("[T]he Client for this campaign was emphatic that her identity would be kept anonymous . . .").

⁴⁸ *Id.* at 2, 7, 13-14.

⁴⁹ *Id.* at 2, 4, 6, 15.

⁵⁰ 47 U.S.C. § 503(b).

⁵¹ 47 CFR § 1.80.

⁵² *The Commission's Forfeiture Policy Statement and Amendment of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines*, Report and Order, 12 FCC Rcd 17087 (1997) (*Forfeiture Policy Statement*), *recons. denied*, Memorandum Opinion and Order, 15 FCC Rcd 303 (1999).

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

⁵⁴ *Notice Response* at 1-2, 5.

assigned to HomeyTel, a company managed by Braun.⁵⁵ The caller ID information selected by Moser was inaccurate in that it represented a phone number that was not assigned to Moser or Marketing Support Systems, and it was misleading in that the chosen caller ID information did not represent a number associated with—or traceable to—Moser.

12. The first prong of the analysis required by Truth in Caller ID Act is satisfied when an entity knowingly causes a caller ID service to transmit inaccurate or misleading caller ID information.⁵⁶ The Commission has determined that “knowingly” modifies the action of the person or entity engaged in malicious caller ID spoofing.⁵⁷ Here, there is no question (and Moser does not contest) that he knowingly spoofed caller ID information. Moser admits to selecting a specific phone number, 619-223-1022, for use in the robocalling campaign.⁵⁸ Moser also admits that: (1) the number was not registered to him or Marketing Support Systems, (2) he did not have permission to use the number,⁵⁹ and (3) he set the caller ID information to display 619-223-1022 through the third-party dialing platform he used to transmit the robocalls.⁶⁰ As a result, rather than displaying the name and contact information for Moser (or even of the client Moser claims hired him to conduct the robocalling campaign), the caller ID on recipients’ phones read 619-223-1022, a number belonging to HomeyTel and untraceable to Moser.⁶¹ Moser admits that he knew the number had belonged to HomeyTel.⁶² HomeyTel did not authorize Moser to use its number,⁶³ and Moser did not claim he had permission from HomeyTel or any other entity to use the number.

13. Moser, however, argues that he did not violate the Truth in Caller ID Act because he “honestly thought [the number] was no longer in use.”⁶⁴ This misses the point. The issue is not whether the number was in use, but whether Moser had a right to use the number. He did not, and he knew it. Moser does not deny that the caller ID information was inaccurate and misleading, nor does he claim that a call recipient could identify or reach the true entity that placed the robocalls. We therefore uphold the findings in the *Notice* that Moser knowingly engaged in spoofing.

B. Moser Made Thousands of Spoofed Robocalls with the Intent to Cause Harm and Wrongfully Obtain Something of Value.

14. The Truth in Caller ID Act prohibits caller ID spoofing when it is done with the intent to “defraud, cause harm, or wrongfully obtain anything of value[.]”⁶⁵ The Commission has held that the

⁵⁵ See, e.g., *id.* at 1-2 (admitting to using a number associated with HomeyTel because of its history of making “hard hitting political calls”). We note that Moser attempts to shift blame for the spoofing violations at issue in this *Order* to his purported client. See *id.* at 8. But Moser admits that he selected the spoofed number and caused it to transmit to call recipients. See *id.* at 5 (admitting to choosing HomeyTel’s phone number for his calling campaign).

⁵⁶ 47 U.S.C. § 227(e); see also 47 CFR § 64.1604.

⁵⁷ *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, Report and Order, WC Docket No. 11-39, 26 FCC Rcd 9114, 9120, para. 17 (2011) (*Truth in Caller ID Order*).

⁵⁸ Notice Response at 5-6.

⁵⁹ See *id.* at 2, 5-6.

⁶⁰ *Id.*

⁶¹ See Fair Political Practices Commission, Case No. 18/336, Declaration of Conrad Braun at 1 (June 13, 2018) (Fair Political Practices Declaration) (Braun testifying that his name and number appeared to recipients of Moser’s calls); see also Notice Response at 2, 5-6 (admitting to using a spoofed number that he knew had belonged to HomeyTel).

⁶² Notice Response at 6 (“The Order states that MSS knew that the phone number used in the campaign, 619-223-1022, was known to us from a lawsuit we filed and won against HomeyTel et al in 2012, which is true.”).

⁶³ Braun Decl.

⁶⁴ Notice Response at 1, 5, 11, 13.

⁶⁵ 47 U.S.C. § 227(e)(1).

element of “harm” in the Truth in Caller ID Act is broad and “encompasses financial, physical, and emotional harm[.]”⁶⁶ Courts have recognized that direct evidence of specific intent is rarely available.⁶⁷ Therefore, it is reasonable and often necessary to look at a party’s actions to determine the party’s intent regarding a wrongful action.⁶⁸ Although Moser asserts that the facts in the cases relied upon by the Commission are inapplicable to the TCPA,⁶⁹ he offers no support for why the principle expressed in them is not applicable here. The principle that conduct may, and often must, be used to assess intent is not dependent on specific facts. The legal principle that we derive from these cases is consistent with our reasoning in past enforcement actions⁷⁰ and well-established federal common law.⁷¹ We therefore reiterate our determinations that conduct may be used to infer an intent to cause harm and that “harm” encompassed by the Truth in Caller ID Act should be read expansively.⁷²

15. Moser acted illegally by (1) failing to provide the requisite identifying information for any of his calls and (2) failing to obtain prior express consent for his calls to wireless numbers. We find that Moser’s spoofing, coupled with these TCPA violations, is indicative of Moser’s intent to cause harm both to HomeyTel and to consumers who received his calls. We also find that he intended to wrongfully obtain something of value by concealing his identity (and avoiding potential lawsuits) through spoofed caller ID information and accepting monetary payment for his unlawful robocalling campaign.

⁶⁶ See *Truth in Caller ID Order*, 26 FCC Rcd at 9122, para. 22; see also *Roesel Forfeiture Order*, 33 FCC Rcd at 9218-19, paras. 39-40.

⁶⁷ *United States v. Dearing*, 504 F.3d 897, 901 (9th Cir. 2007); *United States v. Marabelles*, 724 F.2d 1374, 1379 (9th Cir. 1984); see also *General Cigar Co., Inc. v. CR Carriers, Inc.*, 948 F. Supp. 1030, 1036 (M.D. Ala. 1996) (“Because one cannot know another’s subjective intent, circumstantial evidence must be relied upon to indicate intent. The requirement of specific intent under the mail fraud statute is satisfied by the existence of a scheme which was reasonably calculated to deceive persons of ordinary prudence and comprehension and this intention is shown by examining the scheme itself.”) (internal citations omitted).

⁶⁸ See *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).

⁶⁹ Notice Response at 8-9.

⁷⁰ See, e.g., *Affordable Enterprises of Arizona, LLC*, Notice of Apparent Liability, 33 FCC Rcd 9233, 9242, para. 25 nn.65-66 (2018) (*Affordable Notice*); *Roesel Forfeiture Order*, 33 FCC Rcd at 9213, para. 24 nn.66-67.

⁷¹ The cases reflect holdings of the federal appellate courts of the Fourth, Sixth, Eighth, and Ninth Circuits. *Supra* notes 67-68.

⁷² See *Affordable Notice*, 33 FCC Rcd at 9242, para. 25; *Roesel Forfeiture Order*, 33 FCC Rcd at 9213, para. 24.

1. Moser Intended to Harm the Spoofed Number's Subscriber, HomeyTel

16. Moser intentionally chose a number that he knew was associated with a long-time business rival⁷³ with whom Moser shared a bitter, litigious history⁷⁴—and he admits in his response that he did so.⁷⁵ HomeyTel markets itself as a legitimate company offering legal robocalling services to political candidates.⁷⁶ By spoofing HomeyTel's phone number to make unlawful robocalls, Moser damaged HomeyTel's business reputation and threatened its goodwill to potential customers.

17. We find that Moser intended to cause this harm. 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 intended to harm HomeyTel.⁷⁷ Further, the robocalling campaign led to an immediate backlash against the number's owner (HomeyTel and Braun).⁷⁸ HomeyTel received numerous irate calls from aggrieved call recipients, demanding that the company “stop sending me these disgusting voicemails”⁷⁹ and “stop calling my number,”⁸⁰ and questioning “why are you [autocalling] me with false information.”⁸¹ One particularly enraged consumer left a voicemail message with HomeyTel, explicitly stating: “I don't want you calling me back,” and adding, “*You guys [at HomeyTel] are despicable pieces of sh**.*”⁸² HomeyTel and Braun were also threatened with “imminent litigation” via a cease-and-desist letter sent by Graham (the subject of the robocalling message), who erroneously believed that HomeyTel was behind the unlawful

⁷³ Notice Response at 1-3, 5-6, 8, 11, 13. HomeyTel Network was formerly incorporated in California as “HomeyTel” prior to the suspension of HomeyTel's registration to do business in California. *See* HomeyTel, Articles of Incorporation, Cal. Sec. of State (Mar. 22, 2006). In litigation between Moser and Braun, Braun referred to his business as HomeyTel, Inc. *See, e.g., Moser v. Braun*, Case No. 37-2015-00322367-SC-SC-CTL (filed June 8, 2015). The fact that Braun referred to HomeyTel as HomeyTel, Inc. in the past but now refers to the business as HomeyTel Network is immaterial. The same number that was registered to HomeyTel while it was incorporated in the U.S. is still assigned to HomeyTel Network to the present day. *See* Notice Response at 7 (showing that the HomeyTel, Inc. phone number is registered to HomeyTel Network); Braun Decl. Thus, HomeyTel Network and HomeyTel, Inc., are mere business names of the same entity, HomeyTel, which Braun has continuously managed since 2004 and whose number Moser spoofed. *See* Fair Political Practices Declaration.

⁷⁴ *See, e.g., Moser v. Braun*, Case No. 37-2015-00322367-SC-SC-CTL (filed June 8, 2015) (alleging fraud, breach of settlement, and TCPA violations); *Moser v. HomeyTel et al.*, Case No. 37-2012-00005170-SC-SC-CTL (filed Aug. 29, 2012) (alleging TCPA and Truth in Caller ID Act violations against HomeyTel); *Moser v. Braun et al.*, Case No. 37-2008-00004053-SC-SC-CTL (filed May 29, 2008) (alleging TCPA violations).

⁷⁵ Notice Response at 6 (“The Order states that MSS knew that the phone number used in the calling campaign, 619-223-1022, was known to us from a lawsuit we filed and won against HomeyTel et al in 2012, which is true.”).

⁷⁶ *Home Page*, HomeyTel, http://homeytelblog.com/Home_Page.html (last visited Oct. 8, 2020).

⁷⁷ Complaint #1307215 (Nov. 3, 2016) (on file in EB-TCD-18-00028267).

⁷⁸ *See, e.g., Hiltachk Letter*.

⁷⁹ E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 9, 2019, 16:32 EST) (on file in EB-TCD-18-00028267) (attaching voice mail from{[redacted]} to HomeyTel (May 31, 2018)).

⁸⁰ E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 7, 2019, 16:33 EST) (on file in EB-TCD-18-00028267) (attaching voice mail from{[redacted]} to HomeyTel (May 31, 2018)).

⁸¹ E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 7, 2019, 17:32 EST) (on file in EB-TCD-18-00028267) (attaching voice mail from {[redacted]} to HomeyTel (May 30, 2018)).

⁸² E-mail from Conrad Braun, Operations Manager, HomeyTel, to Sonja Rifken, Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (Feb. 7, 2019, 16:11 EST) (on file in EB-TCD-18-00028267) (attaching voice mail from {[redacted]} to HomeyTel (May 30, 2018)) (emphasis added).

robocalling campaign.⁸³ Moser caused the victims of the illegal robocalling campaign to misdirect their outrage and complaints towards HomeyTel rather than Moser or his client. Based on the record, we find that this harm was both reasonably foreseeable and intentional.

18. Moser knew that the phone number he selected for the caller ID had been associated with HomeyTel. And the evidence contradicts Moser's claim that he was not aware that the number still belonged to HomeyTel, which he contends is a "defunct" business entity.⁸⁴ *First*, Moser knew or should have known that the number was still assigned and in service because he stated that his calls went to voicemail when he called that number.⁸⁵ Voicemail requires a phone line to be active and in service; thus, if Moser tested the number to see if it was active, as he claims to have done, the voicemail response made it obvious that the line was in service. *Second*, although HomeyTel was no longer registered in the United States after 2015, HomeyTel continued to operate in Mexico and it updated the company's contact information on its publicly available website.⁸⁶ *Third*, HomeyTel updated the copyright date on its website multiple times after 2015, which evinces additional business-related activity.⁸⁷ Moser knew the number was active, knew that it was or had been associated with HomeyTel, and chose the number *because* of its association with HomeyTel. Moser questions the validity of Braun's affidavits, specifically Braun's contention that HomeyTel is currently an operating business entity.⁸⁸ We verified the content of Braun's affidavits through other sources⁸⁹ and relied on the affidavits only to establish: (1) that HomeyTel was the subscriber of the called number and (2) that Moser did not have permission to use that number. Moser's intentional conduct and personal history with Braun and HomeyTel indicates that Moser intended to harm them both.⁹⁰

19. Even if we were not convinced that Moser intended to harm HomeyTel specifically, we nonetheless would find that he intended to harm any current or future subscriber to the number he spoofed. Where, as here, a caller uses a spoofed number as part of an illegal robocalling campaign, the harm is not merely potential, but actual and certain.⁹¹ Moser admits that he intentionally chose a spoofed

⁸³ Hiltachk Letter.

⁸⁴ Moser alleges that, regardless of what the caller ID depicted, he did not believe that the phone number he selected was still registered to HomeyTel or Braun. Notice Response at 11. However, we do not find Moser's evidence persuasive. *Compare id.* at 1, 5, 11 (arguing that HomeyTel is a defunct corporation), *with id.* at 7 (admitting he is aware that, since 2016, Braun and his wife "receive not only their personal mail but also [] receive payments for both HomeyTel Inc and HomeyTel Network[,]," which also affirms that HomeyTel conducts business operations and is, therefore, a functioning business entity).

⁸⁵ *Id.* at 11.

⁸⁶ *HomeyTel Home Page*, WaybackMachine, https://web.archive.org/web/20170706062343/http://homeytelblog.com/Home_Page.html (last visited Oct. 8, 2020) (*2017 Webpage*) (showing that by 2017 HomeyTel had updated its website to reflect its new contact information and location in Ensenada, Mexico).

⁸⁷ *Compare 2017 Webpage*, *with HomeyTel Home Page*, WaybackMachine, https://web.archive.org/web/20180825094157/http://homeytelblog.com/Home_Page.html (last visited Oct. 8, 2020) (showing that HomeyTel updated its content copyright date in 2017 and 2018 before Moser spoofed the company's number).

⁸⁸ Notice Response at 2-3, 5-6, 14-15.

⁸⁹ *See* Letter from Kristi Thompson, Division Chief, Telecommunications Consumer Division, FCC Enforcement Bureau, to { [] } (Mar. 4, 2019) (on file in EB-TCD-18-00028267); BNA Response (confirming that HomeyTel has been a subscriber of Vonage since 2015); Call Detail Records.

⁹⁰ Moser's arguments concerning Braun's allegedly unlawful activities and credibility are irrelevant to this action and are not a defense to Moser's unlawful conduct.

⁹¹ *See, e.g., Roesel Forfeiture Order*, 33 FCC Rcd at 9215-16, para. 33 n.85.

number to display on the caller ID of the unlawful robocalls.⁹² Moser's actions harmed the present and future usefulness of the number—regardless of whether it was used by HomeyTel or some other subscriber—by associating it with thousands of illegal robocalls that disturbed and enraged the recipients of his calls. Moser recognized that the robocalls were likely to generate controversy, anger, and even lawsuits.⁹³ Thus, Moser knew that many consumers would want to respond to the calls, and their efforts to reach the caller would result in the number's rightful subscriber being inundated with complaints. Moser claims that he selected the number because it was already associated with “hard hitting political call[]” campaigns.⁹⁴ But that does not negate his intent to cause harm. At most, it shows that he intended to cement that phone number's association with political robocalling activities.

2. Moser Intended to Harm the Recipients of His Spoofed Robocalls

20. Accurate caller ID information allows called parties to decide whether they should answer the phone and trust the entity making the call. The Commission has found that spoofing, when done in conjunction with an illegal robocalling campaign, can indicate an intent to cause harm.⁹⁵ All of Moser's 47,610 calls failed to provide accurate caller ID information, and we find that Moser intended to harm consumers by hiding the identity of the caller.

21. The TCPA requires that prerecorded message calls include the phone number of the entity responsible for initiating the call.⁹⁶ Moser did not include the phone number or true identity of the calling party in the May 2018 calls.⁹⁷ Staff listened to the voice file provided by the third-party dialing platform, and it failed to mention any phone number at all.⁹⁸ The only identification information referenced “Jennifer Jones” as the sponsor of the call, which Moser admitted was a pseudonym⁹⁹ because

⁹² See Notice Response at 5 (“[W]e choose [sic] to use what we honestly thought was an old phone number of a now long defunct California [c]orporation[,] HomeyTel”); *id.* at 11 (“[Moser] honestly and reasonably believed this phone number to be a ‘dead’ corporate VOIP phone number, as it belonged to a defunct corporation. It is no longer answered by an employee as it was previously because it apparently [] no longer employs anyone and now just goes straight to voicemail.”).

⁹³ See *id.* at 5 (“As stated[,] the Client for this campaign was emphatic that her identity would be kept anonymous as she feared the exact type of political retribution MSS has now received and potentially worse.”); *id.* at 12 (“Our client was insistent that her identity be kept confidential, as she feared reprisal from a politically connected individual.”); *id.* (“[O]ur only intent was to fulfil[] our client[]’s need and desire to remain anonymous.”). Moser, himself, believes that he was harmed on multiple occasions when he received unwanted robocalls. See, 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 July 12, 2017); *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 (filed Oct. 23, 2015); *Engle, Moser v. Unified Life Insurance Co., Inc., et al.*, Case No. 14-CV-1908-MMA-JLB (S.D. CA filed Aug. 13, 2014).

⁹⁴ Notice Response at 2. Although Moser contends that he spoofed the 619-223-1022 number because of its history making political calls, Braun stated that the number is not used for political robocalls and is only used for soliciting new business. Fair Political Practices Declaration at 2. Regardless, by spoofing a number to further embed its reputation for “hard hitting” partisan robocalling, Moser demonstrated an intent to harm the current and future owners of that number.

⁹⁵ *Roesel Forfeiture Order*, 33 FCC Rcd at 9218-19, paras. 40-41; *Roesel Notice*, 32 FCC Rcd at 6408, para. 16.

⁹⁶ 47 U.S.C. § 227(d)(3)(A). Moser does not dispute that he initiated the calls. We make no finding, for purposes of liability under the TCPA, concerning whether Moser's client also could be found to have made the calls, as it is irrelevant to the case at hand.

⁹⁷ Dialing Platform Response at File PHILGRAHAM_REV_VO.MP3.

⁹⁸ *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.

⁹⁹ Notice Response at 5.

“[the client] chose not to reveal her identity in her message”¹⁰⁰ Moser’s spoofing went hand-in-hand with his refusal to identify the caller, as required by the TCPA. Had the calls included legitimate caller ID information, the called parties would have had a better opportunity to identify the caller and decide whether to answer the phone. Legitimate caller ID information also would have permitted called parties to contact Moser and object to the calls.

22. The record demonstrates that Moser is well aware of the requirements of the TCPA. As an initial matter, because Moser’s company, Marketing Support Systems, is a telemarketing services provider,¹⁰¹ he is presumptively familiar with the requirements and restrictions of the TCPA.¹⁰² That presumption is confirmed by the fact that Moser has also filed or participated in more than 15 complaints alleging TCPA violations in the courts,¹⁰³ including complaints that allege that robocallers sent prerecorded voice messages to his wireless phone number in violation of the TCPA.¹⁰⁴ In one of his lawsuits, Moser contended that he was harmed in a variety of ways by receiving 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 service . . . the costs of having to pursue legal remedies, and in the aggravation and consequent health effects of stress these illegal intrusions have caused.¹⁰⁵

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”¹⁰⁶ Thus, Moser has admitted that he relies on caller ID information to determine whether to answer a call and that receiving illegal, spoofed robocalls can cause significant harm, including aggravation and stress. We find that Moser’s actions in this case demonstrate that he was aware of and intended to cause the very harms he describes.

23. The TCPA also requires that the prerecorded message clearly identify the entity that made the call and provide a callback number for the entity.¹⁰⁷ Moser claims that neither he nor his client were required to identify themselves in the automated message due to California campaign finance rules for independent expenditures under \$1,000.¹⁰⁸ Compliance with state election law, however, is not relevant here. Moser may not hide behind state law to evade compliance with federal law: The

¹⁰⁰ *Id.*

¹⁰¹ See Better Business Bureau, *Marketing Support Systems Profile*, <https://www.bbb.org/us/ca/san-diego/profile/telemarketing-services/marketing-support-systems-1126-1014054> (last visited Oct. 8, 2020); 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 Oct. 8, 2020).

¹⁰² See *United States v. Int’l Minerals & Chem. Corp.*, 402 U.S. 558, 563 (1971) (“The principle that ignorance of the law is no defense applies whether the law be a statute or a duly promulgated and published regulation.”); see also *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.”).

¹⁰³ *Supra* notes 30-32 (providing examples of Moser’s TCPA litigation).

¹⁰⁴ *Moser v. Health Insurance Innovations, Inc. et al.*, Case No. 17-CV-1127-WQH-KSC (S.D. CA) (filed June 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.

¹⁰⁵ *Moser v. Health Insurance Innovations, Inc. et al.*, at para. 96.

¹⁰⁶ *Moser v. Health Insurance Innovations, Inc. et al.*, at para. 97.

¹⁰⁷ 47 U.S.C. § 227(d)(3)(A).

¹⁰⁸ Notice Response at 5; see Cal. Gov’t Code § 84310 (West 2018).

California law might not require the candidate to identify herself, but it does not prohibit it.¹⁰⁹ Moreover, the California law only exempts from its identification and disclosure rules the person or entity that “paid for the call[.]” not the third-party that places the calls.¹¹⁰ Thus, Moser (as the caller) needed to identify himself in the messages under the TCPA, and such identification would not conflict with the California law.

24. The placement of unlawful robocalls causes consumers significant harm, including that such calls are a nuisance and an invasion of privacy.¹¹¹ The TCPA prohibits transmitting prerecorded voice messages to wireless phones unless the called party has provided prior express consent or the call is for an emergency purpose.¹¹² This robocall restriction applies to “any call” to a wireless number regardless of the content of the call,¹¹³ which includes calls made for a “political purpose.”¹¹⁴ Moser’s calls were thus covered by the prior express consent requirement.

25. 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.¹¹⁵ Moser failed to obtain consent from the wireless robocall recipients. 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 or “Jennifer Jones” permission to robocall them. Of the 44 people with whom Bureau staff spoke, not a single person stated that they had granted Moser, Marketing Support Systems, and/or “Jennifer Jones” permission to call them on their wireless phone; nine affirmatively stated that they did not.¹¹⁶ Moser offers no proof of prior express consent.

26. Instead, Moser argues that when applicants “knowingly gave their phone numbers” to register to vote, they were consenting to receive Moser’s political robocalls.¹¹⁷ He therefore claims that he obtained consent from the robocall recipients when he solicited their phone numbers from the San Diego Registrar of Voters and signed an affidavit stating that he would use the numbers for a permissible purpose.¹¹⁸

27. Moser overstates and misconstrues the scope of the consent provided by registered voters. *First*, the mere act of providing one’s phone number to the government for voter registration purposes does not create express consent to receive unsolicited robocalls and certainly does not establish

¹⁰⁹ Cal. Gov’t Code § 84310(a).

¹¹⁰ *Id.* We make no determination as to whether Moser or his client complied with California law.

¹¹¹ See *Roesel Forfeiture Order*, 33 FCC Rcd at 9218, para. 40.

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

¹¹³ 47 U.S.C. § 227(b)(1)(A).

¹¹⁴ See *Biennial Reminder for Political Campaigns About Robocall and Text Abuse, Enforcement Advisory*, Public Notice, 31 FCC Rcd 1940, 1941 (2016) (*Biennial Political Robocall Reminder*); see also *Barr v. Am. Assoc. of Political Consultants, Inc.*, 140 S.Ct. at 2344 (“[P]laintiffs still may not make political robocalls to cell phones [under the TCPA].”). Calls with a “political purpose” are not part of the class of calls exempted from 47 U.S.C. § 227(b)(1)(A) under 47 U.S.C. § 227(b)(2)(C).

¹¹⁵ Dialing Platform Response at Call Detail Records.

¹¹⁶ Declaration of { [redacted] } (filed Apr. 5, 2019) (on file in EB-TCD-18-00028267); Declaration of { [redacted] } (filed Mar. 27, 2019) (on file in EB-TCD-18-00028267).

¹¹⁷ See Notice Response at 12.

¹¹⁸ See *id.*; see also County of San Diego Registrar of Voters, Application for Voter Registration Information (2018) (on file in EB-TCD-18-00028267).

consent to receive robocalls from a third-party unknown to the call recipient. Any consent given is not transferrable to an unaffiliated third-party.¹¹⁹

28. *Second*, the voter registration forms upon which Moser relies do not include the consent that Moser needed under the TCPA. The San Diego Registrar of Voters obtained its voter log from two sources¹²⁰—the National Mail Voter Registration Form¹²¹ and the California state voter registration application.¹²² The National Mail Voter Registration Form states only that “[m]ost States ask for your telephone number *in case there are questions about your application*. However, you do not have to fill in this box.”¹²³ The form does not indicate that, by providing one’s number, the applicant consents to receive robocalls from an unknown third-party. The only use of an applicant’s phone number articulated on the state application is that applicants’ “[p]hone numbers are posted at polling places on election day.”¹²⁴ Thus, the call recipients who provided their numbers to the government for voter registration purposes did not expressly consent to receive robocalls on their phones.

3. Moser Falsified Caller ID Information with the Intent to Wrongfully Obtain Something of Value

29. The Act and the Commission’s rules make it unlawful to spoof caller ID information with the “intent to defraud, cause harm, or wrongfully obtain anything of value[.]”¹²⁵ The Commission has found that “anything of value” applies to both tangible and intangible benefits.¹²⁶ This interpretation is consistent with similar turns of phrase in other contexts. In a criminal embezzlement case, for instance, the Second Circuit described the phrase “thing of value” as “words of art . . . [T]he phrase is generally construed to cover intangibles as well as tangibles. For example, amusement is held to be a thing of value under gambling statutes.”¹²⁷ Moser argues that the violations depicted in the cases cited by the

¹¹⁹ See *GroupMe, Inc./Skype Communications S.A.R.L. Petition for Expedited Declaratory Ruling, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Declaratory Ruling, 29 FCC Rcd 3442, 3447, para. 14 (2014) (*GroupMe Declaratory Ruling*) (“[W]e confirm that a caller remains liable for TCPA violations when it relies upon the assertion of an intermediary that the consumer has given such prior express consent. We emphasize that the intermediary may only convey consent that has actually been provided by the consumer; the intermediary cannot provide consent on behalf of the consumer.”); see also *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, P2P Alliance Petition for Clarification*, CG Docket No. 02-278, Declaratory Ruling, 35 FCC Rcd 6526, 6530, para. 13 (CGB 2020) (*P2P Declaratory Ruling*) (affirming that “‘persons who knowingly release their telephone numbers’ for a particular purpose . . . [consent] to be called . . . for that purpose[.]”) (emphasis added).

¹²⁰ See E-mail from Michael Vu, Registrar, San Diego Registrar of Voters, to Brandon Thompson, Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau (June 25, 2020, 14:17 EDT) (on file in EB-TCD-18-00028267).

¹²¹ U.S. Election Assistance Comm., National Voter Registration Application Form for U.S. Citizens, https://www.eac.gov/sites/default/files/eac_assets/1/6/Federal_Voter_Registration_ENG.pdf (last visited Oct. 8, 2020) (*National Mail Voter Registration Form*).

¹²² Cal. Secretary of State, *Classification - Voter Registration Application*, <https://covr.sos.ca.gov/?step=2> (last visited Oct. 8, 2020).

¹²³ *National Mail Voter Registration Form* at 2 (emphasis added).

¹²⁴ Cal. Secretary of State, *Classification - Voter Registration Application*, <https://covr.sos.ca.gov/?step=2> (last visited Oct. 8, 2020) (select “[I am a] U.S. citizen and resident of California,” then click “Next”).

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

¹²⁶ See, e.g., *Roesel Forfeiture Order*, 33 FCC Rcd at 9218, para. 39.

¹²⁷ *United States v. Girard*, 601 F.2d 69, 71 (2nd Cir. 1979) (citations omitted); see also *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”); accord *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);

Commission are not robocall violations, therefore, the courts' interpretations of the phrase "anything of value" are inapplicable to the present case.¹²⁸ While the facts of these cases vary, the legal issue—how to define the scope of the phrase "anything of value" or "thing of value"—is the same. The Commission's interpretation of "anything of value" in this case is supported by the cited case law and is consistent with Commission precedent.¹²⁹ In *Roesel*, for example, we found that "anything of value" included using spoofing to secure a client's business or marketing leads and was not limited to gaining something of value from the call recipients themselves.¹³⁰

30. The evidence shows that Moser intended to wrongfully obtain something of value from his illegal spoofing campaign. Specifically, Moser sought to: (1) evade both law enforcement and consumer litigation, and thereby avoid culpability, and (2) benefit monetarily from making unlawful, spoofed robocalls.¹³¹

31. Moser argues that the case law cited by the Commission does not prove that intent can be determined through circumstantial evidence such as conduct.¹³² However, Moser later admits that conduct may be indicative of intent.¹³³ Moreover, courts have held that intent frequently must be deduced from conduct.¹³⁴ Moser also argues that he "stood to gain nothing" from the calls, but he again contradicts himself by admitting that he received compensation for making the calls, and engaged in unlawful spoofing to secure his client's business¹³⁵—both of which are "things of value."¹³⁶

32. *Liability Shield*. Moser spoofed HomeyTel's number with the intent to gain a valuable liability shield from detection and culpability.¹³⁷ The Commission may impose a penalty of up to \$20,489

United States v. Draves, 103 F.3d 1328 (7th Cir. 1997) (agreeing with and applying Fifth Circuit's expansive interpretation of phrase "anything of value" in *Picquet*); *United States v. Nilsen*, 967 F.2d 539, 542-43 (11th Cir. 1992) ("Congress' frequent use of 'thing of value' in various criminal statutes has evolved the phrase into a term of art which the courts generally construe to envelope both tangibles and intangibles. This broad interpretation is based upon a recognition that monetary worth is not the sole measure of value."); *United States v. Schwartz*, 785 F.2d 673, 680 (9th Cir. 1986) (noting 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).

¹²⁸ Notice Response at 8-9, 12.

¹²⁹ See, e.g., *Roesel Forfeiture Order*, 33 FCC Rcd at 9218, para. 39.

¹³⁰ *Id.* at 9216, paras. 34-35.

¹³¹ Notice Response at 4.

¹³² *Id.* at 9.

¹³³ *Id.* at 11 ("We accept it is necessary and reasonable to look at a party's actions to determine the party's intent regarding a wrongful action.").

¹³⁴ See *supra* notes 67-68.

¹³⁵ Notice Response at 5 ("[T]he Client for this campaign was emphatic that her identity would be kept anonymous as she feared the exact type of political retribution MSS has now received and potentially worse. Thus[,] to protect our Client, we choose to use [a spoofed number].").

¹³⁶ See *supra* note 127.

¹³⁷ *Roesel Forfeiture Order*, 33 FCC Rcd at 9212, para. 22; *Roesel Notice of Apparent Liability*, 32 FCC Rcd at 6413, para. 27 ("Avoidance of culpability is a benefit that qualifies as a thing of value."). HomeyTel suffered some of the legal action and backlash that Moser would have faced had he not used spoofed caller ID. See Hiltachk Letter.

for each violation of the TCPA,¹³⁸ which would be in addition to liabilities arising out of any private actions.¹³⁹ If a court finds that the defendant in such a private right of action willfully or knowingly violated the TCPA or its implementing rules, the court may award up to \$1,500, treble damages, per violation to the plaintiff.¹⁴⁰

33. Moser knew that violating the TCPA brought with it the potential for civil liability. He conducts telemarketing and/or telephone outreach for a living and is often a private litigant in TCPA cases himself. Moser argues that he could not have intended to avoid liability because he was not subject to potential liability in the first place. His contention that he could not be held not liable was neither accurate nor reasonable. *First*, Moser had no reason to believe that political robocalls are exempt from the TCPA.¹⁴¹ *Second*, he had no basis for assuming that he could not be held liable because he used a spoofed number at his client's request.¹⁴² He argues that his client was the sole party responsible for the robocalls and therefore should be solely liable, while he acted as a mere messenger.¹⁴³ But the Commission has found that both the entity that initiates a call and that entity's client may be held mutually liable for violations of the TCPA.¹⁴⁴ Regardless of who created the prerecorded voice message, it was Moser who selected the call recipients, placed the calls, and caused a caller identification service to transmit misleading and inaccurate caller ID information by selecting and using a number that did not belong to him or his client.¹⁴⁵ Spoofing was not the only avenue available for Moser if his sole intention was to protect his client's identity. He could have conducted the calling campaign without divulging the identity of his client by simply using a number assigned to him or his company as the caller ID. Instead, spoofing provided Moser a liability shield for himself and delayed his detection by law enforcement. Therefore, we find that Moser intended to shield himself from liability and culpability for violations of the TCPA and thus wrongfully obtain something of value.

34. *Financial Compensation.* Moser admits to accepting financial compensation to conduct the unlawful robocalling scheme.¹⁴⁶ In *Roesel*, we found that, at a minimum, "anything of value" includes obtaining money to conduct the unlawful activity.¹⁴⁷ Moser states that his client emphatically insisted that

¹³⁸ See 47 U.S.C. § 503(b)(2)(D); *Amendment of Section 1.80(b) of the Commission's Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, 34 FCC Rcd 12824 (EB 2019).

¹³⁹ 47 U.S.C. § 227(b)(3).

¹⁴⁰ *Id.* § 227(b)(3)(C).

¹⁴¹ See *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 27 FCC Rcd 1830, 1831, para. 3 (2012) (*2012 TCPA Report and Order*). Political robocalls to wireless phones are subject to the TCPA's private right of action. See *Biennial Political Robocall Reminder*, 31 FCC Rcd at 1941. ("These provisions apply to all such prerecorded voice calls and autodialed calls or texts, including those made by political campaigns or other organizations . . .").

¹⁴² See Notice Response at 2 ("We [spoofed the caller ID] at the request of our client so as to protect her identity as she wanted to remain anonymous fearing retribution which was her right."); *id.* at 15 ("Our clear intent was not to injure but to . . . provide anonymity to our client for all the reasons stated. We're not so foolish in this digital age as to think that these calls could not be traced but didn't think anyone would bother for an exempt political message.").

¹⁴³ *Id.* at 6.

¹⁴⁴ See *Dialing Services, LLC*, Forfeiture Order, 32 FCC Rcd 6192, 6199-200, para. 21 (2017) ("As the Commission stated in the [Notice], and as set forth explicitly in the *DISH Network* [ruling], both a seller (or client, in this case) who engages a telemarketer (or robocaller, in this case) and the telemarketer (or robocaller) so engaged, may be liable for TCPA violations."); *Joint Petition filed by DISH Network LLC*, CG Docket No. 11-50, Declaratory Ruling, 28 FCC Rcd 6574, 6583, para. 27 (2013).

¹⁴⁵ Notice Response at 2, 5 (admitting to causing a spoofed caller ID to display on recipients' phones).

¹⁴⁶ *Id.* at 4, 13.

¹⁴⁷ *Roesel Notice*, 32 FCC Rcd at 6413, para. 25, *aff'd*, *Roesel Forfeiture Order*, 33 FCC Rcd at 9212, para. 22.

he keep her identity a secret; Moser chose to meet this demand by selecting a spoofed caller ID.¹⁴⁸ Therefore, we find that Moser benefited monetarily from making unlawful, spoofed robocalls.

C. All Robocalls are Subject to the Requirements of the TCPA

35. Our determination that Moser violated the Truth in Caller ID Act rests, in part, on our finding that Moser demonstrated, through his noncompliance with the TCPA, an intent to harm and an intent to wrongfully obtain something of value. Moser contends that political calls are not subject to liability under the TCPA.¹⁴⁹ But neither the TCPA nor the Truth in Caller ID Act exempt political calls from the obligations at issue here.¹⁵⁰ Under the express terms of the TCPA, all robocalls made to wireless numbers for non-emergency purposes—regardless of content—must satisfy certain requirements, which include obtaining prior express consent from call recipients and providing the name and a callback number of the calling entity.¹⁵¹ And to the degree that Moser implies that political speech warrants different treatment under the TCPA as a constitutional matter, the Supreme Court just months ago concluded that it does not.¹⁵²

36. The TCPA is not limited to telemarketing calls but, rather, includes non-commercial calls and calls made for political purposes. The Commission has held that political robocalls and other noncommercial robocalls are regulated by the Telephone Consumer Protection Act (TCPA).¹⁵³ The Commission has also issued guidance on several occasions to remind political campaigns and organizations that, although we do not regulate the *content* of political robocalls,¹⁵⁴ political robocalling is nonetheless governed by the TCPA and our rules.¹⁵⁵ Accordingly, we reject Moser’s claim that the TCPA does not regulate non-commercial robocalls, including those with a “political purpose.”¹⁵⁶

¹⁴⁸ Notice Response at 2 (“We did this at the request of our client”); *id.* at 5 (“[T]he client for this campaign was emphatic that her identity would be kept anonymous Thus to protect our Client, we [used a spoofed number.]”); *id.* at 12 (stating that Moser intended to fulfill his client’s desire to remain anonymous).

¹⁴⁹ *Id.* at 7-8, 10, 15.

¹⁵⁰ Noncommercial robocallers need not obtain prior consent to make calls to wireline phones. 47 U.S.C. § 227(b)(2)(B)(i). However, noncommercial robocallers must obtain prior express consent before making calls to wireless numbers and adhere to the TCPA’s identification requirements. *Id.* § 227(b)(1)(A)(iii), (d)(3). Noncommercial robocalls are also governed by the Truth in Caller ID Act. *Id.* § 227(e).

¹⁵¹ *Id.* § 227(b)(1)(A); *id.* § 227(d)(3)(A)(i)-(ii).

¹⁵² *Barr v. Am. Assoc. of Political Consultants, Inc.*, 140 S.Ct. 2335, at 2344 (2020) (“As a result, plaintiffs still may not make political robocalls to cell phones, but their speech is now treated equally with debt-collection speech.”). “The implicit premise of [Plaintiff’s] argument is that extending the robocall restriction to debt-collection robocalls would be unconstitutional. But that is wrong. A generally applicable robocall restriction would be permissible under the First Amendment. Extending the robocall restriction to those robocalls raises no First Amendment problem.” *Id.* at 2355 (upholding the constitutionality of the TCPA).

¹⁵³ *2012 TCPA Report and Order*, 27 FCC Rcd at 1831, para. 3 (“None of our actions change requirements for prerecorded messages that are non-telemarketing, informational calls, such as . . . calls for political purposes Such calls continue to require some form of prior express consent under the TCPA and the Commission’s rules, if placed to wireless numbers and other specified recipients.”).

¹⁵⁴ *Biennial Political Robocall Reminder*, 31 FCC Rcd at 1941 (“[The TCPA’s] broad prohibition covers prerecorded voice and autodialed calls, including those sent by nonprofit or political campaign-related organizations.”); Federal Communications Commission, *Political Campaign Robocalls & Robotexts*, <https://www.fcc.gov/political-campaign-robocalls-robotexts> (last visited Oct. 8, 2020).

¹⁵⁵ 47 U.S.C. § 227(b)-(d); 47 CFR § 64.1200.

¹⁵⁶ Notice Response at 8, 10, 12-13. Moser states, for example, that “not for profit political messages which are protected 1st Amendment speech [are] exempt from the TCPA per §227(a)(4).” *Id.* at 10. However, Moser later admits that the TCPA does, in fact, place restrictions on robocalls made with a political purpose. *Id.* at 13 (stating

D. The Commission’s Forfeiture is Based Solely on Moser’s Illegal Spoofing, Not the Content of the Political Message

37. The Commission’s forfeiture decision is based on Moser’s unlawful spoofing in violation of the Truth in Caller ID Act, not the veracity of the prerecorded voice message.¹⁵⁷ Moser argues that when he made the calls, he did not know that the allegations against Graham had been dismissed.¹⁵⁸ Moser also argues that his calls parroted information that had already been reported by news media.¹⁵⁹ These arguments do not alter our finding that Moser spoofed caller ID with wrongful intent. The Commission’s action does not hinge on the truthfulness or factual accuracy of the prerecorded message or Moser’s knowledge thereof. In fact, our decision makes no determination about the impact that the calls had on Graham’s campaign or whether Moser (or his client) intended to harm Graham. Our decision rests only on the use of spoofed caller ID in conjunction with an intent to cause harm to HomeyTel and consumers, and Moser’s use of spoofing to wrongfully obtain something of value.

38. Moser asserts that “[t]he FCC . . . appears to be trying to regulate the content of political speech.”¹⁶⁰ To the contrary, our decision is based on Moser’s unlawful spoofing and is not dependent on the content of the call.¹⁶¹ Moser argues that, because the Commission described Moser’s conduct as “egregious,” the Commission must have been referring to the content of the calls.¹⁶² But the Commission’s reference to “egregious” behavior referred to Moser’s spoofing-related conduct, not the content of the message.¹⁶³ We thus reject Moser’s assertion that the Commission’s action is based on the content of the prerecorded message.¹⁶⁴ Because the violations at issue in the *Notice* did not relate to the content of the robocalling messages, Moser’s First Amendment rights are not implicated.¹⁶⁵

E. The Full Amount of the Forfeiture is Warranted

39. When we assess forfeitures, we must take into account 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.”¹⁶⁶ After considering the relevant statutory factors and the Commission’s *Forfeiture Policy Statement*,¹⁶⁷ we find that Moser is liable for a

his opinion that “[t]he restrictions placed by the TCPA and the FCC’s application thereof are over-inclusive and pose too great a threat to the freedom of speech”).

¹⁵⁷ *Notice*, 34 FCC Rcd at 12755, para. 6 n.12; *id.* at 12760, para. 18.

¹⁵⁸ *Notice Response* at 5.

¹⁵⁹ *Id.* at 13.

¹⁶⁰ *Id.* at 10.

¹⁶¹ The *Notice* did not refer to the content of the calls in its legal analysis; it only described the messages in the Background section. *Notice*, 34 FCC Rcd at 12753, para. 1.

¹⁶² *Notice Response* at 13.

¹⁶³ *Notice*, 34 FCC Rcd at 12763-65, paras. 29-35. Specifically, we found that an upward adjustment of the base forfeiture total was necessary because Moser egregiously and intentionally spoofed the number of a business rival whom he knew personally, and because Moser had spoofed HomeyTel’s number before.

¹⁶⁴ *Notice Response* at 13.

¹⁶⁵ Even if the First Amendment is implicated here, which we dispute, the TCPA is a content-neutral restriction on speech. Moser does not argue that his speech was restricted by the Truth in Caller ID Act.

¹⁶⁶ 47 U.S.C. § 503(b)(2)(E).

¹⁶⁷ *The Commission’s Forfeiture Policy Statement and Amendment of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines*, Report and Order, 12 FCC Rcd 17087 (1997) (*Forfeiture Policy Statement*), *recons. denied*, Memorandum Opinion and Order, 15 FCC Rcd 303 (1999).

total forfeiture of \$9,997,750.¹⁶⁸ Our investigation determined that Moser made 47,610 illegally spoofed calls.¹⁶⁹ Of those, we evaluated 5,713 calls, all of which were made to wireless phones, and determined that each of those calls was made using a phone number assigned to HomeyTel without HomeyTel's consent.¹⁷⁰ Our forfeiture results from applying a \$1,000 base forfeiture to the 5,713 spoofed calls to wireless phones and then applying an upward adjustment of 75%.¹⁷¹

1. The Commission's Evidence Supports the Forfeiture

40. The Commission based its investigation and proposed forfeiture in this case on facts and other credible evidence. Moser does not contest the amount of the forfeiture or seek a reduction. He contends, however, that the Commission's findings and proposed forfeiture are a "political prosecution"¹⁷² that relies upon the declaration and court filings of Conrad Braun and ignores the weight of the evidence as a whole.¹⁷³

41. Moser's contentions are unfounded. We note at the outset that we verified the content of Braun's affidavit through other sources.¹⁷⁴ More fundamentally, the forfeiture is based on facts and admissions in the record, a fair amount of which Moser himself supplied to us. HomeyTel was the subscriber of the number displayed in the robocalling campaign,¹⁷⁵ Moser was aware of that fact, and Moser also knew he did not have permission to use that number. In addition, Moser was in a good position to understand the monetary benefits of serving his client as well as the benefits of evading liability for TCPA violations. Our findings in this investigation are based on Moser's own knowing and deliberate actions. We take no cognizance of the content of the prerecorded messages here because that content is irrelevant to our analysis. Weighing the relevant statutory factors, the evidence before us, and our own forfeiture guidelines, we conclude that the proposed forfeiture of \$9,997,750 properly reflects the seriousness and scope of Moser's violations.

2. The Commission Satisfied Moser's Fifth Amendment Due Process Rights

42. Moser's contention that his constitutional due process rights have been disregarded is ill-founded. Under the Communications Act, a party engaged in apparently unlawful spoofing is entitled to receive a notice of apparent liability that informs the recipient of the government's proposed action, including its finding that the recipient is apparently liable for specified violations.¹⁷⁶ A notice of apparent

¹⁶⁸ 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.

¹⁶⁹ We note that we could have assessed a penalty for all 47,610 calls, regardless of whether their destination was a wireless phone or landline phone—all 47,610 calls are spoofing violations under the Truth in Caller ID Act. *See* 47 U.S.C. § 227(e) (choosing not to differentiate between landline and wireless phones for the purpose of determining whether a violation occurred).

¹⁷⁰ *See Notice*, 34 FCC Rcd at 12756, para. 8.

¹⁷¹ *See id.* at 12758, para. 13.

¹⁷² Notice Response at 1, 15. Moser's accusation that our findings are a "political prosecution" on behalf of a "political prince" is meritless. The Commission began its investigation based on a referral from the Office of Alex Padilla, a Democrat and the California Secretary of State, to look into a complaint brought to the Secretary's attention by Graham, a Republican.

¹⁷³ *Id.* at 14.

¹⁷⁴ *See supra* note 89.

¹⁷⁵ *See Braun Decl.*; *see also* Letter from Kristi Thompson, Division Chief, Telecommunications Consumer Division, FCC Enforcement Bureau, to {[]} (Mar. 4, 2019) (on file in EB-TCD-18-00028267); BNA Response (confirming that HomeyTel is subscriber).

¹⁷⁶ 47 U.S.C. § 227(e)(5)(A)(iii); 47 U.S.C. § 503(b)(1)(B); *Notice*, 34 FCC Rcd at 12766, para. 38 (informing Moser of his right to file a written response should he wish to contest the *Notice*).

liability serves to alert the party to our preliminary analysis and to grant it an opportunity to respond before the Commission takes final action. We adhered to this process in the present case, and Moser availed himself of his right to respond.

43. Nevertheless, Moser claims that the Commission failed to warn that the *Notice* was in the offing.¹⁷⁷ Moser provides no legal support for his contention that a warning was required, and in fact, there is no such requirement. To the contrary, when enacting section 227(e) to address the harms of illegal spoofing, Congress expressly empowered the Commission “to proceed expeditiously” on the basis of a proper notice alone,¹⁷⁸ and the Commission already has determined that it is not obligated to “first issue a non-monetary warning in the form of a citation.”¹⁷⁹ For apparent violations of the Truth in Caller ID Act, the Commission wields discretion to provide either: (1) notice and an opportunity for a hearing before the Commission or an administrative law judge¹⁸⁰ or, as in this case, (2) a written notice of apparent liability and an opportunity for a written response.¹⁸¹

44. The Commission also provided Moser with all of the information and documents that the agency relied upon in the *Notice*, as well as additional non-material documents that did not inform our proposed determination and sanction but which we had permission to disclose.¹⁸² We did not, however, release nonpublic information to Moser that we are barred by rule from disclosing.¹⁸³ In other words, the Commission has provided all the process to him that is due.

45. Moser nonetheless argues that he is entitled to the “entire investigative file,” including non-public records and all documents upon which the Commission did *not* rely.¹⁸⁴ In an attempt to locate, among other things, non-existent exculpatory evidence and non-public (and not relied upon) information, Moser filed Freedom of Information Act (FOIA) requests in connection with this investigation.¹⁸⁵ Moser argues that he is entitled to all communications between the Commission and third-parties in relation to this matter and is unable to prepare a proper response to the Commission’s *Notice* until he receives a response to his FOIA request.¹⁸⁶

46. We disagree with Moser on the need to delay our forfeiture decision until he receives additional documents beyond those we already have furnished. As a matter of fact, the Commission has

¹⁷⁷ Notice Response at 7 (Moser arguing that the Commission was required to contact him before issuing its *Notice*).

¹⁷⁸ 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. *See* 47 U.S.C. § 227(e)(5)(A).

¹⁷⁹ *Truth in Caller ID Order*, 26 FCC Rcd at 9132, para. 47.

¹⁸⁰ *See* 47 U.S.C. § 503(b)(3).

¹⁸¹ *See id.* § 503(b)(4).

¹⁸² *See* E-mail from Shana Yates, Deputy Division Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Kenneth Moser, Owner, Marketing Support Systems (Apr. 17, 2020, 16:59 EDT) (on file in EB-TCD-18-00028267).

¹⁸³ 47 CFR § 19.735-203(a).

¹⁸⁴ Notice Response at 13-14. Moser also argues that the Brady Rule requires that the Commission disclose any materially exculpatory evidence. *Id.* at 14. *See generally Brady v. Maryland*, 373 U.S. 83 (1963) (requiring that prosecutors disclose exculpatory evidence to criminal defendants). However, the Brady Rule only applies to federal criminal law cases, not administrative actions.

¹⁸⁵ Notice Response at 14.

¹⁸⁶ *Id.*

disposed of both of his FOIA requests relating to this matter.¹⁸⁷ But even if those requests were still pending, we would not need to delay our forfeiture decision any further. The FOIA requests and this enforcement action are distinct and independent proceedings. In general, neither the identity of the party making a document request under FOIA or the purpose of that request has any bearing on the merits of the request.¹⁸⁸ Moser's rights under FOIA thus are no different from those of any member of the public who requests information under that statute. More generally, a FOIA request does not implicate due process rights absent a showing that the requested information is material or presents a substantial basis to claim materiality.¹⁸⁹ No such showing has been made here.

47. In sum, the Commission in this case—consistent with its practice in enforcement matters—has provided to Moser all relevant documents and information that served as the basis for the *Notice*. Moreover, Commission staff also analyzed his FOIA requests on a timely basis and, although the FOIA requests had no bearing on his deadline for responding to the *Notice*, provided Moser with substantial extensions of time to submit his Notice Response.¹⁹⁰ Accordingly, we find that the Commission's *Notice* conformed with due process requirements.

IV. ORDERING CLAUSES

48. Accordingly, **IT IS ORDERED** that, pursuant to section 503(b) of the Act,¹⁹¹ and section 1.80 of the Commission's rules,¹⁹² Kenneth Moser, doing business as Marketing Support Systems, **IS LIABLE FOR A MONETARY FORFEITURE** in the amount of nine million, nine hundred ninety-seven thousand, seven hundred and fifty dollars (\$9,997,750) for willfully and repeatedly violating section 227(e) of the Act¹⁹³ and section 64.1604 of the Commission's rules.¹⁹⁴

49. Payment of the forfeiture shall be made in the manner provided for in section 1.80 of the Commission's rules within thirty (30) calendar days after the release of this Forfeiture Order.¹⁹⁵ Moser shall send electronic notification of payment to Lisa Williford, Enforcement Bureau, Federal Communications Commission, at lisa.williford@fcc.gov on the date said payment is made. If the forfeiture is not paid within the period specified, the case may be referred to the U.S. Department of Justice for enforcement of the forfeiture pursuant to section 504(a) of the Act.¹⁹⁶

50. Payment of the forfeiture must be made by credit card, ACH (Automated Clearing House) debit from a bank account using the Commission's Fee Filer (the Commission's online payment

¹⁸⁷ See E-mail from Stacey Weiss, Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau, to Kenneth Moser, Owner, Marketing Support Systems (May 19, 2020, 8:28 EDT); see also E-mail from Stacey Weiss, Attorney Advisor, Telecommunications Consumers Division, FCC Enforcement Bureau, to Kenneth Moser, Owner, Marketing Support Systems (June 8, 2020, 15:40 EDT).

¹⁸⁸ *United States Department of Justice v. Reporters Committee for Freedom of Press*, 489 U.S. 749, 771 (1989).

¹⁸⁹ *United States v. Agurs*, 427 U.S. 97, 196 (1976).

¹⁹⁰ See E-mail from Shana Yates, Deputy Division Chief, Telecommunications Consumers Division, FCC Enforcement Bureau, to Kenneth Moser, Owner, Marketing Support Systems (May 6, 2020, 13:22 EDT) (on file in EB-TCD-18-00028267).

¹⁹¹ 47 U.S.C. § 503(b).

¹⁹² 47 CFR § 1.80.

¹⁹³ 47 U.S.C. § 227(e).

¹⁹⁴ 47 CFR § 64.1604.

¹⁹⁵ *Id.* § 1.80.

¹⁹⁶ 47 U.S.C. § 504(a).

system),¹⁹⁷ or by wire transfer. The Commission no longer accepts forfeiture payments by check or money order. Below are instructions that payors should follow based on the form of payment selected:¹⁹⁸

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

51. Any request for making full payment over time under an installment plan should be sent to: Chief Financial Officer – Financial Operations, Federal Communications Commission, 45 L Street NE, Washington, DC 20554.¹⁹⁹ Questions regarding payment procedures should be directed to the Financial Operations Group Help Desk by telephone, 1-877-480-3201, or by e-mail ARINQUIRIES@fcc.gov.

52. **IT IS FURTHER ORDERED** that a copy of this Forfeiture Order shall be sent by first class mail and certified mail, return receipt requested, to Kenneth Moser dba Marketing Support Systems at 11280 Spica Drive, San Diego, CA 92126.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

¹⁹⁷ Payments made using the Commission’s Fee Filer system do not require the submission of an FCC Form 159.

¹⁹⁸ For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #6), or by e-mail at ARINQUIRIES@fcc.gov.

¹⁹⁹ See 47 CFR § 1.1914.

**STATEMENT OF
CHAIRMAN AJIT PAI**

Re: *Kenneth Moser dba Marketing Support Systems*, File No.: EB-TCD-18-00028267.

Approximately one week before California's 2018 primary election, tens of thousands of residents of the 76th State Assembly District in San Diego County were bombarded with robocalls. In these calls, a prerecorded voice message graphically described an alleged sexual assault involving a candidate for an open State Assembly seat—an allegation that turned out to be false.

An investigation by our Enforcement Bureau identified Kenneth Moser as the originator of these 47,610 calls. None of these calls contained accurate caller ID information. Instead, Moser changed the caller ID information so that the calls appeared to come from a company called HomeyTel Network, which just happened to be a business rival of Moser's.

These calls violated the Truth in Caller ID Act of 2009, and today the Commission formally imposes a \$9,997,750 forfeiture on Moser.

None of Moser's objections to our decision today have any merit. For example, Moser claims that he didn't intend for his spoofing to harm HomeyTel because he thought that the company was no longer using the phone number that he inserted into the caller ID information. But this contention isn't credible. Moser intentionally chose to use a phone number that he knew belonged to a business rival with whom he had a bitter, litigious history. One would have to be rather naïve to think that this was not done with the intent to cause harm. And not only did Moser intend to cause HomeyTel harm, he actually did harm, as the company bore the brunt of angry complaints from many who received the robocalls.

Moser also argues that he is not subject to liability because the robocalls in question were political in nature. No luck there either. The Truth in Caller ID Act doesn't exempt political calls from its requirements. Put simply, political campaigns do not have carte blanche to make robocalls with inaccurate caller ID information.

I want to thank our staff for conducting a meticulous and dogged investigation that once again has allowed us to bring a spoofer to justice: Lisa Gelb, Rosemary Harold, Jermaine Haynes, Shannon Lipp, Latashia Middleton, Tanishia Proctor, Nakasha Ramsey, Linda Simms, Kristi Thompson, Brandon Thompson, Kimberly Thorne, Bridgette Washington, Lisa Williford, Shana Yates, and Lisa Zaina of the Enforcement Bureau; Eduard Bartholme, Kurt Schroeder, Mark Stone, and Kristi Thornton of the Consumer and Governmental Affairs Bureau; Valerie Hill, Rick Mallen, and Bill Richardson of the Office of General Counsel; Alex Espinoza and Rachel Kazan of the Office of Economics and Analytics; and Daniel Kahn and Melissa Droller Kirkel of the Wireline Competition Bureau.

**STATEMENT OF
COMMISSIONER MICHAEL O'RIELLY,
APPROVING IN PART AND DISSENTING IN PART**

Re: *Kenneth Moser dba Marketing Support Systems*, File No.: EB-TCD-18-00028267.

Those familiar with my approach to similar forfeiture proceedings know that I am strongly committed to a text-based interpretation of the Truth in Caller ID Act's prohibitions on spoofing. While we should certainly take swift and meaningful enforcement action against those who violate the statute, we shouldn't twist the words of the Act to achieve a preferred result or an outcome that aligns with certain political priorities.

As a result, I've departed from the Commission in previous enforcement proceedings that found a subject's intent to cause harm despite the absence of probative evidence to indicate a malevolent mindset. For better or for worse, the statute requires a finding of "intent," and often, the facts simply don't support such a finding. Similarly, I disagree with this item's claim that Moser's spoofing campaign, in conjunction with his TCPA violations, are on their own indicative of an intent to harm the called parties. Rather, he intended to disseminate negative information about a candidate for political office during a primary election on an anonymous basis, pursuant to his client's wishes. In other words, he falsified caller ID not to harm the call recipients, but to engage in anonymous speech, a type of interest that the Supreme Court has deemed to be protected under the First Amendment, including in an election context.¹

While I disagree that Moser intended to harm the recipients of his calls, the record does support the finding that he intended to harm his competitor HomeyTel by spoofing a number assigned to it, and I therefore approve with respect to that part of the draft. However, I completely disagree with the item's finding that, even if there weren't sufficient evidence that Moser intended to harm his competitor, he nevertheless intended to harm any current or future subscriber to the number he spoofed. If that's true, spoofing itself is always determinative of an intent to cause harm (after all, there are always going to be potential current or future subscribers to a number), which would render the "intent" prong of the statute totally meaningless.

Further, I am grateful that, unlike the NAL, the Forfeiture Order does not focus unnecessarily on the "falsity" of the information in the calls, which is irrelevant to our analysis. The FCC shouldn't give the impression that we are targeting a caller on the basis of content, regardless of the ultimate grounds for liability. I appreciate that the item before us doesn't repeat some of the more sensationalist language from the NAL (i.e., "egregious"; "smeared a political candidate"; and "factually baseless"), and I hope that our future enforcement proceedings will make every effort not to repeat this previous error.

I approve in part and dissent in part.

¹ See *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995).

**STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL**

Re: *Kenneth Moser dba Marketing Support Systems*, File No.: EB-TCD-00028267.

You're tired of them. Me too. The calls that tumble in every day, offering a cruise or debt relief or something else you did not ask for, do not want, and do not need—they are exasperating. Robocalls are degrading communications and destroying trust in networks. And after a brief downturn in the volume of these calls during the early days of the pandemic, scammers are back at it. The numbers are going up.

We need to respond in kind. With more action, more enforcement, and more penalties—like what we do here today. In this decision we impose a forfeiture against a caller who used the spoofed numbers of a competitor to make tens of thousands of calls to spread misinformation about a political campaign. This was sordid stuff. One week before a state primary, this robocall campaign featured allegations about sexual assault by a candidate that ultimately resulted in the accuser pleading guilty to making a false report of a crime. The California Secretary of State referred this matter to us for investigation. We did just that and as a result this order has my full support. But it is not the only calling campaign that needs investigation. Just two weeks ago there were reports that millions of robocalls were also using spoofed numbers to spread misinformation in advance of the November election. This, too, needs attention. Because if these calls ran afoul of the tools we have to protect consumers—like the Telephone Consumer Protection Act, Truth in Caller ID Act, and TRACED Act—this agency needs to act.