



**REPORT TO CONGRESS**

**ON**

**ROBOCALLS AND TRANSMISSION OF MISLEADING OR INACCURATE  
CALLER IDENTIFICATION INFORMATION**

**Prepared by the:**

**Enforcement Bureau, Consumer and Governmental Affairs Bureau, and  
Wireline Competition Bureau**

**Submitted pursuant to Sections 3, 11, and 13 of the Pallone-Thune Telephone Robocall  
Abuse Criminal Enforcement and Deterrence Act**

**December 23, 2020**

The Federal Communications Commission (FCC or Commission) files this report pursuant to Sections 3, 11, and 13 of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act).<sup>1</sup> Section 3 of the TRACED Act amended the Telephone Consumer Protection Act (TCPA) in several respects.<sup>2</sup> This report provides the information that Section 3 requires, including data regarding informal consumer complaints that the Commission received during the preceding five full calendar years (2015-2019), and Commission enforcement actions during the preceding calendar year (2019). We also provide additional informal consumer complaint data and information about Commission enforcement actions through November 30, 2020.

Sections 11 and 13 address certain Commission and private industry actions with respect to illegal robocalls as defined in 47 U.S.C. §§227(b) and (e), including unsolicited calls using an artificial or prerecorded voice message, often referred to as “robocalls.”<sup>3</sup> This report covers the period from December 1, 2019 through November 30, 2020.

### **Telephone Consumer Protection Act**

Section 227(b) restricts calls using an automatic telephone dialing system or an artificial or prerecorded voice.<sup>4</sup> It prohibits calls to residential phones if the call uses an artificial or prerecorded voice message, unless the called party consents or the call is for an emergency purpose or falls within other enumerated exceptions.<sup>5</sup> Absent coverage by a relevant exception, such calls are illegal robocalls. The provision also places restrictions on unsolicited advertisements to facsimile machines, known as “junk faxes.”<sup>6</sup>

Section 227(c) directs the Commission to initiate a rulemaking proceeding to protect residential telephone subscribers’ privacy rights to avoid receiving telephone solicitations to which they object. The section also provides a private right of action to persons that receive more than one telephone call within any 12-month period by or on behalf of the same entity in violation of the TCPA.<sup>7</sup>

Section 227(d) prohibits using a telephone facsimile machine, or automatic telephone dialing system, that does not comply with the technical and procedural standards outlined in the TCPA. This section prohibits the use of a computer or other electronic device to send any message via a telephone facsimile machine unless such person clearly marks, in a margin at the top or bottom of each transmitted page of the message or on the first page of the transmission, the date and time it is sent and an

---

<sup>1</sup> Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133 Stat. 3274 (2019) (TRACED Act). The Commission consulted with the Federal Trade Commission on this report, as provided in section 3 of the TRACED Act.

<sup>2</sup> Section 227 of the Communications Act of 1934, as amended, is designed to protect consumers from unsolicited, unlawful calls by restricting autodialed or pre-recorded message calls and unsolicited facsimiles, and by minimizing transmission of misleading or inaccurate caller ID information. *See* 47 U.S.C. §§ 227(b)-(e).

<sup>3</sup> *See* 47 U.S.C. §§ 227(b) and (e).

<sup>4</sup> 47 U.S.C. § 227(b)(1)(A).

<sup>5</sup> 47 U.S.C. § 227(b)(1)(B).

<sup>6</sup> *See* 47 U.S.C. § 227(b)(1)(C). Under this provision unsolicited advertisements to facsimile machines are prohibited unless the party receiving the facsimile has a preexisting business relationship with the sender, has consented to receive the facsimile, or has agreed to make available its facsimile number for public distribution. However, there are limitations to these exceptions.

<sup>7</sup> 47 U.S.C. § 227(c)(1) and (5).

identification of the business.<sup>8</sup> This section also requires that all artificial or prerecorded telephone messages shall clearly state at the beginning of the call the identity of the entity initiating the call, and during or after the call the telephone number or address of the entity.<sup>9</sup>

Section 227(e), also known as the Truth in Caller ID Act, prohibits “caus[ing] any caller identification service” in connection with any voice service or text message service to “knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value[.]”<sup>10</sup> Such practices are known as “spoofing.”

### **Section 3 of the TRACED Act**

Section 3 of the TRACED Act amends the TCPA in several respects that affect Commission enforcement. First, the TRACED Act removes the requirement that the Commission issue a citation, or warning, pursuant to section 503(b)(5) of the Communications Act before the Commission may propose a monetary forfeiture under section 227(b).<sup>11</sup> Second, Section 3 prescribes an additional potential monetary penalty for violations of section 227(b) if the Commission determines that the person acted “with the intent to cause such violation.”<sup>12</sup> Third, Section 3 sets a four-year statute of limitations period in which the Commission may take enforcement action against intentional violations of section 227(b); previously the statute of limitations was one year.<sup>13</sup> Fourth, Section 3 sets a four-year statute of limitations period in which the Commission may take enforcement action against violations of section 227(e); previously the statute of limitations was two years.<sup>14</sup> On May 1, 2020, the Commission released an order amending section 1.80 of its rules in accordance with the amendments that Section 3 made to Section 227(b) of the Communications Act.<sup>15</sup>

Section 3(h) of the TRACED Act requires the Commission to submit an annual report, following consultation with the Federal Trade Commission. The information required by Section 3(h) is as follows:

#### **The Number of Consumer Complaints Alleging a Violation of 227(b)-(e)**

From January 1, 2015 through November 30, 2020, the Commission has received 368,584 informal consumer complaints alleging a violation of 227(b), 644,495 informal consumer complaints alleging a violation of 227(c), 280,769 informal consumer complaints alleging a violation of 227(d), and 213,818 informal consumer complaints alleging a violation of 227(e).

---

<sup>8</sup> 47 U.S.C. § 227(d)(1).

<sup>9</sup> 47 U.S.C. §227(d)(3).

<sup>10</sup> 47 U.S.C. § 227(e); *see also* 47 CFR § 64.1604. The prohibition does not apply to “lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States; or [to a]ctivity engaged in pursuant to a court order that specifically authorizes the use of caller identification manipulation.” 47 CFR § 64.1604(b); *see also* 47 U.S.C. § 227(e)(3)(B)(ii); 47 U.S.C. § 227(e)(7).

<sup>11</sup> *See* TRACED Act § 3(a)(1)(4)(A)-(B), 133 Stat. at 3274.

<sup>12</sup> *Id.* § 3(a)(1)(4)(B), 133 Stat. at 3274. Such amounts are recoverable under section 504(a) of the Communications Act. *See* 47 U.S.C. § 504(a).

<sup>13</sup> *See* 47 CFR § 1.80(c)(4).

<sup>14</sup> *See* 47 CFR § 1.80(c)(3).

<sup>15</sup> *See Amendment of Section 1.80 of the Commission’s Rules; Implementing Section 3 of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, Order, 35 FCC Rcd 4476, para. 6 (EB 2020).

The chart below provides the total number of informal consumer complaints received by the Commission by calendar year alleging violations of 227(b) through 227(e) from January 1, 2015 through November 30, 2020. It is important to note that one complaint may contain several violations covered by 227 (b)-(e) and may be counted multiple times. For example, complaints alleging spoofed caller ID prohibited under 227(e) may also be robocall violations under 227(b) or Do Not Call violations under 227(c) and thus might be listed up to three times in the following chart.

Year	227(b)	227(c)	227(d)	227(e)
2015	48,436	90,616	56,599	15,783
2016	40,694	79,015	47,081	12,169
2017	84,978	136,845	68,562	26,199
2018	100,104	146,730	47,915	38,397
2019	58,797	106,698	34,992	70,866
2020*	35,575	84,591	25,620	50,404

\*2020 complaints from January 1, 2020 through November 30, 2020.

#### Citations to enforce §227(d)

The Commission issued two citations to enforce §227(d) during the preceding calendar year (2019).<sup>16</sup>

1. *Dante Sciarra and D&D Global Enterprises, LLC*.—On November 27, 2019, the Commission issued a citation and order notifying Dante Sciarra and D&D Global (D&D) that they violated the law by sending prerecorded solicitations, without identification, to wireless numbers—some of which were registered on the Do-Not-Call Registry.<sup>17</sup> During a four-month period, D&D made thousands of calls per day alerting call recipients that their business listings might be at risk of not being seen on Google and other online directories.<sup>18</sup> The citation directed D&D to take immediate steps to comply with the Communications Act and informed it that failure to comply with the TCPA may result in liability for significant fines.<sup>19</sup>
2. *Kenneth Moser dba Marketing Support Systems*.—On December 13, 2019, the Commission issued a citation and order notifying Kenneth Moser (Moser) that he violated the law by making unauthorized and disruptive prerecorded voice message calls without the required identification information, and to wireless phone numbers without an emergency purpose or consent.<sup>20</sup> Moser made thousands of prerecorded message calls to residents of the California 76th State Assembly District in San Diego County.<sup>21</sup> The messages described criminal allegations against one of eight candidates for a vacant State Assembly seat.<sup>22</sup> The citation directed Moser to take immediate

<sup>16</sup> See list of FCC citations in edocs database (<https://www.fcc.gov/tags/citation>).

<sup>17</sup> See *Dante Sciarra and D&D Global Enterprises, LLC*, Citation and Order, 34 FCC Rcd 11210, 11211 (2019).

<sup>18</sup> See *id.*

<sup>19</sup> See *id.*

<sup>20</sup> See *Kenneth Moser dba Marketing Support Systems*, Citation and Order, 34 FCC Rcd 11969 (2019).

<sup>21</sup> See *id.* at 11970.

<sup>22</sup> See *id.* at 11969.

steps to comply with the Communications Act and informed him that failure to comply with the TCPA may result in liability for significant fines.<sup>23</sup>

### **Notices of Apparent Liability for Forfeiture**

The Commission issued one notice of apparent liability during the preceding calendar year (2019) to enforce §§227(b)-(e).

1. *Kenneth Moser dba Marketing Support Systems.*—On December 13, 2019, the Commission proposed a forfeiture of \$9,997,750 for apparent violations of the Truth in Caller ID Act.<sup>24</sup> Kenneth Moser, doing business as a telemarketing enterprise under the name Marketing Support Systems (Moser), apparently made 47,610 unlawful spoofed calls over the course of a two-day calling campaign.<sup>25</sup> Moser apparently spoofed the phone number assigned to another telemarketing company, HomeyTel, Inc. (HomeyTel), to transmit a prerecorded voice message containing false statements critical of California State Assembly candidate Philip Graham.<sup>26</sup> Moser apparently is not affiliated with HomeyTel and not authorized to use its phone number.<sup>27</sup> To the contrary, he apparently has had a long and contentious relationship with HomeyTel and that company's founder and current manager, Conrad Braun.<sup>28</sup> As a result of the apparently spoofed calls, HomeyTel received a multitude of complaints from recipients of the prerecorded voice message call, as well as a cease-and-desist letter from the candidate referenced in the message.<sup>29</sup>

The Commission issued two notices of apparent liability between January 1, 2020 through November 30, 2020 to enforce §§227(b)-(e).

1. *Scott Rhodes.*—On January 31, 2020, the Commission proposed a forfeiture of \$12,910,000 for apparent violations of the Truth in Caller ID Act. Scott Rhodes (Rhodes) apparently made more than 6,000 unlawful spoofed robocalls between May 2018 and December 2018.<sup>30</sup> Rhodes apparently altered his caller ID information to appear as local numbers as part of his campaign to send provocative prerecorded voice message calls. The Commission identified six distinct calling campaigns, each of which targeted voters in districts during political campaigns or residents in communities that had experienced major news events relating to or involving white nationalism, immigration, or other public controversies.
2. *John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman.*—On June 10, 2020, the Commission proposed the largest fine in FCC history: \$225,000,000. John C. Spiller and Jakob A. Mears, doing business under the names

---

<sup>23</sup> See *id.*

<sup>24</sup> See *Kenneth Moser dba Marketing Support Systems*, Notice of Apparent Liability for Forfeiture, 34 FCC Rcd 12753 (2019).

<sup>25</sup> See *id.*

<sup>26</sup> See *id.*

<sup>27</sup> See *id.*

<sup>28</sup> See *id.*

<sup>29</sup> See *id.*

<sup>30</sup> See *Scott Rhodes a.k.a. Scott David Rhodes, Scott D. Rhodes, Scott Platek, Scott P. Platek*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 882, 882 (2020).

Rising Eagle Capital Group LLC, JSquared Telecom LLC, Only Web Leads LLC, Rising Phoenix Group, Rising Phoenix Holdings, RPG Leads, and Rising Eagle Capital Group – Cayman (collectively, Rising Eagle), made approximately one billion spoofed robocalls in the first four-and-a-half months of 2019 with the apparent intent to defraud, cause harm, and wrongfully obtain something of value in apparent violation of the Truth in Caller ID Act.<sup>31</sup>

### **Forfeiture Orders**

The Commission did not issue any forfeiture orders in the preceding calendar year (2019). It issued two forfeiture orders between January 1, 2020 through November 30, 2020 for violations of §§227(b)-(e).

1. *Affordable Enterprises of Arizona, LLC*.—On October 29, 2020, the Commission adopted an order imposing a \$37,525,000 forfeiture fine on Affordable Enterprises of Arizona, LLC (Affordable) for making unlawfully spoofed telemarketing calls to consumers throughout Arizona—many of whom had placed their numbers on the National Do Not Call Registry to avoid unwanted telemarketing calls.<sup>32</sup> When making the calls, Affordable did not transmit the actual originating phone number.<sup>33</sup> Instead, Affordable displayed the caller ID information of: (1) numbers that were assigned to prepaid wireless phones, for which the subscriber information was not available; (2) numbers that were unassigned (i.e., not in use by any consumer); or (3) numbers that were assigned to consumers who had no affiliation or relationship with Affordable.<sup>34</sup> Over a 14-month period spanning 2016 and 2017, Affordable made 2,341,125 unlawful spoofed telemarketing calls.<sup>35</sup> Calls were made by spoofing numbers that were, at the time of the calls, either unassigned or assigned to innocent consumers—leaving such individuals vulnerable to scores of angry callbacks from other consumers whom Affordable had targeted with unwanted marketing messages while effectively shielding itself from their complaints.<sup>36</sup>
2. *Kenneth Moser dba Marketing Support Systems*.—On November 18, 2020, the Commission adopted an order imposing a \$9,997,750 forfeiture fine on Kenneth Moser (Moser), doing business as Marketing Support Systems, for violating section 227(e) of the Communications Act of 1934, as amended,<sup>37</sup> and section 64.1604 of the Commission’s rules.<sup>38</sup> Moser admitted to intentionally spoofing a phone number assigned to HomeyTel Network (HomeyTel), a long-time business rival.<sup>39</sup> 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 was not authorized to use HomeyTel’s

---

<sup>31</sup> See *John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948, 5948 (2020).

<sup>32</sup> See *Affordable Enterprises of Arizona, LLC*, Forfeiture Order, 35 FCC Rcd 12142, 12142 (2020).

<sup>33</sup> See *id.*

<sup>34</sup> See *id.*

<sup>35</sup> See *id.*

<sup>36</sup> See *id.*

<sup>37</sup> 47 U.S.C. § 227(e).

<sup>38</sup> 47 CFR § 64.1604.

<sup>39</sup> See *Kenneth Moser dba Marketing Support Systems*, Forfeiture Order, FCC-20-163 (2020).

phone number. Moser has had 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."<sup>40</sup>

### **Forfeiture penalties and criminal fines collected**

The Commission does not collect criminal fines for violations of section 227.

If a party fails to pay a forfeiture, we refer the matter to the U.S. Department of Justice for further prosecution. Our most recent referrals to the Department of Justice regarding forfeiture orders involving violations of section 227 were *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc. (Abramovich)* and *Philip Roesel, dba Wilmington Insurance Quotes, and Best Insurance Contracts, Inc. (Roesel)*. During calendar year 2019, the Attorney General did not collect any forfeiture penalties or criminal fines for violations of section 227 cases that the Commission has referred. We lack knowledge about the U.S. Department of Justice's collections beyond those cases.

### **Proposals for reducing the number of unlawful calls**

The Commission has proposed and implemented a broad range of actions to combat illegal and unwanted robocalls made in violation of §§227(b)-(e), with a focus on giving consumers and carriers the tools necessary to block unwanted robocalls. Below, we highlight the Commission's most recent proposals in three areas: facilitating consumer-driven call blocking, combatting illegal spoofing of robocalls, and stopping specific scams.

1. *Facilitating Consumer-Driven Call Blocking*.—Historically, the Commission has found that call blocking, with limited exceptions, is an unjust and unreasonable practice under section 201(b) of the Act.<sup>41</sup> In November 2017, however, the Commission identified certain, well-defined circumstances in which voice service providers may block calls.<sup>42</sup> Specifically, the Commission authorized providers to block calls purporting to be from numbers on a Do Not Originate list as well as calls where the number purporting to originate the call is invalid, unallocated, or unused.<sup>43</sup> The industry first tested blocking calls in a small Do Not Originate trial that blocked calls that

---

<sup>40</sup> See *id.*

<sup>41</sup> See *Blocking Interstate Traffic in Iowa*, Memorandum Opinion and Order, 2 FCC Rcd 2692 (1987); *Access Charge Reform*, CC Docket No. 96-262, *Seventh Report and Order and Further Notice of Proposed Rulemaking*, 16 FCC Rcd 9923, 9932-33, para. 24 (2001); *Connect America Fund, A National Broadband Plan for Our Future, Establishing Just and Reasonable Rates for Local Exchange Carriers, High-Cost Universal Service Support, Developing a Unified Intercarrier Compensation Regime, Federal-State Joint Board on Universal Service, Lifeline and Link-Up, Universal Service Reform-Mobility Fund*, Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd 17663, 17903, para. 734 (2011); *Rural Call Completion*, WC Docket No. 13-39, Notice of Proposed Rulemaking, 28 FCC Rcd 1569, 1572-73, paras. 7-11 (2013). *But see Total Communications Services, Inc., and Atlas Tel. Co., Inc., v. AT&T*, Memorandum Opinion and Order, 16 FCC Rcd 5726 (2001) (finding that the Act did not prohibit a carrier from blocking calls from its customers to a sham entity designed to impose increased access charges).

<sup>42</sup> See *Advanced Methods to Target and Eliminate Unlawful Robocalls, Report and Order and Further Notice of Proposed Rulemaking*, 32 FCC Rcd 9706, (2017). In addition, the Commission has clarified that nothing in the Communications Act or our rules or orders prohibits consumers from using third-party blocking apps. *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, WC Docket No. 07-135, Declaratory Ruling and Order, 30 FCC Rcd 7961, 8033-38, paras. 152-63 (2015).

<sup>43</sup> Do Not Originate calls are those made from a number that the subscriber does not use to make outgoing calls and requests that calls purporting to originate from that number be blocked.

spoofed specific Internal Revenue Service numbers, which resulted in a significant drop in IRS scam calls.<sup>44</sup> The industry now reports widespread implementation of Do Not Originate blocking, and several voice service providers have implemented or are implementing blocking of invalid, unallocated, and unused numbers.<sup>45</sup> The Commission followed up on this order in December 2018, issuing a declaratory ruling that wireless providers are authorized to stop unwanted text messaging through robotext-blocking, anti-spoofing measures, and other anti-spam features.<sup>46</sup> In June 2019, the Commission clarified that voice service providers may offer by default programs that block illegal and unwanted calls before they reach consumers' phones.<sup>47</sup>

In July 2020, the Commission adopted the *Call Blocking Order and Further Notice*.<sup>48</sup> The *Call Blocking Order* enables more voice-service-provider call blocking by establishing two safe harbors from liability under the Communications Act and the Commission's rules.<sup>49</sup> The first safe harbor protects voice service providers that block calls that they determine are unwanted based on reasonable analytics that take into consideration caller ID authentication information.<sup>50</sup> The second safe harbor protects voice service providers that block calls from bad-actor upstream providers when the upstream providers fail to mitigate bad traffic or take effective steps to prevent new and renewing customers from originating illegal traffic after the Commission has notified them of that traffic.<sup>51</sup> The *Call Blocking Order* also requires voice service providers that block calls to provide a single point of contact for blocking disputes and takes steps to ensure that critical calls are not blocked, consistent with sections 4(c)(1) and 10(b) of the TRACED Act.<sup>52</sup> The *Further Notice* adopted with the *Call Blocking Order* sought comment on additional blocking, along with safeguards against erroneous blocking.

2. *Combatting Illegal Spoofing*.—Caller ID authentication is one way to help consumers identify scams and verify who is calling.<sup>53</sup> The benefits of authentication are substantial: consumers and

---

<sup>44</sup> “The IRS conveyed a 90% reduction in IRS scam call complaints in the last two months, with the largest drop off coinciding with the [DNO] trial, from a high of 43,000 complaints in late August to only 3,700 complaints in mid-October. . . . One [participant] noted a dramatic reduction in numbers associated with the IRS scam crossing their network from 8,000 per day to 1,000.” Robocall Strike Force, Robocall Strike Force Report at 1 (Oct. 26, 2016), <https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf>.

<sup>45</sup> See Consumer and Governmental Affairs Bureau, Federal Communications Commission, Report on Robocalls, CG Docket No. 17-59 (Feb. 14, 2019), para 18, <https://www.fcc.gov/document/report-robocalls> (Robocalls Report).

<sup>46</sup> *Petitions for Declaratory Ruling on Regulatory Status of Wireless Messaging Service*, WT Docket No. 08-7, Declaratory Ruling, 33 FCC Rcd 12075 (2018).

<sup>47</sup> *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876 (2019).

<sup>48</sup> *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614 (2020) (*Call Blocking Order and Further Notice*).

<sup>49</sup> *Id.* at 7623-31 paras. 20-45.

<sup>50</sup> *Id.* at 7625-27, paras. 25-34.

<sup>51</sup> *Id.* at 7627-31, paras. 35-45.

<sup>52</sup> *Id.* at 7633-36, paras. 51-59.

<sup>53</sup> Caller ID authentication, such as STIR/SHAKEN, is technology that enables voice service providers to verify that the caller ID information transmitted with a call matches the caller's phone number. Its widespread implementation



voice service providers will know that callers are who they say they are, thereby reducing the risk of fraud and ensuring that callers can be held accountable for their calls. Authentication has the potential to alleviate harmful forms of spoofing.<sup>54</sup> In July 2017, the Commission launched an inquiry on how to build upon and facilitate industry's work on caller ID authentication.<sup>55</sup> Chairman Pai sent letters to voice service providers in November 2018, demanding that the industry adopt a robust call authentication system and launch that system no later than 2019.<sup>56</sup> He asked providers about their specific implementation plans, and encouraged them to protect their customers without delay by using STIR/SHAKEN, an authentication framework helpful in combating illegal caller ID spoofing.<sup>57</sup>

In August 2019, the Commission adopted new rules banning malicious caller ID spoofing of text messages and foreign calls.<sup>58</sup> These rules implemented Congressional direction in the RAY BAUM'S Act and closed a loophole in the law that prevented the Commission from pursuing scammers sending spoofed text messages and international fraudsters making spoofed calls to Americans.

In March 2020, the Commission mandated that all voice service providers implement STIR/SHAKEN in the IP portions of their networks by June 30, 2021.<sup>59</sup> In September 2020, the Commission adopted the *Second STIR/SHAKEN Order*, which adopted new rules to further implement STIR/SHAKEN and protect consumers against malicious caller ID spoofing.<sup>60</sup> The *Second STIR/SHAKEN Order* clarified the obligations and deadlines for voice service providers regarding caller ID authentication and completed implementation of the TRACED Act's

---

will reduce the effectiveness of illegal spoofing, allowing law enforcement to identify bad actors more easily, and help voice service providers identify calls with illegally spoofed caller ID information before those calls reach their subscribers.

<sup>54</sup> See Robocalls Report, para. 20.

<sup>55</sup> See generally *Call Authentication Notice*.

<sup>56</sup> Press Release, FCC, Chairman Pai Sent Letters To Voice Service Providers In November, Demanding That They Move Forward On Caller ID Authentication (Nov. 5, 2018), <https://www.fcc.gov/document/chairman-pai-demandsindustry-adopt-protocols-end-illegal-spoofing>.

<sup>57</sup> STIR/SHAKEN is an Internet Protocol (IP)-based technology that enables voice service providers to verify that the caller ID information transmitted with a call matches the caller's phone number. More specifically, STIR/SHAKEN confirms that a call actually comes from the number indicated in the caller ID, or at least that the call entered the US network through a particular voice service provider or gateway. Protocols developed by the Secure Telephony Identify Revisited (STIR) working group of the Internet Engineering Task Force (IETF) work with the Signature-based Handling of Asserted information using toKENs (SHAKEN) implementation standards created by the Alliance for Telecommunications Industry Solutions (ATIS) and the SIP Forum. Call Authentication Trust Anchor Working Grp., N. Am. Numbering Council, Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR at 17 (2018), [http://nancchair.org/docs/mtg\\_docs/May\\_18\\_Call\\_Authentication\\_Trust\\_Anchor\\_NANC\\_Final\\_Report.pdf](http://nancchair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf).

<sup>58</sup> *Implementing Section 503 of RAY BAUM'S Act*, WC Docket Nos. 18-335 and 11-39, Second Report and Order, 34 FCC Rcd 7303 (2019).

<sup>59</sup> *Call Authentication Trust Anchor*, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241 (2020) ("*First Caller ID Authentication Report and Order and Further Notice*").

<sup>60</sup> *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, FCC 20-136 (Sept. 29, 2020) (*Second STIR/SHAKEN Order*).

provisions regarding this technology. The rules require voice service providers with non-IP technology to either upgrade their non-IP networks to IP and implement STIR/SHAKEN, or work to develop a non-IP authentication solution. Voice service providers that have not implemented STIR/SHAKEN must establish a robocall mitigation program until they implement the caller ID authentication technology. Finally, intermediate providers must implement STIR/SHAKEN so that IP calls retain caller ID authentication information throughout the entire call path.

The Commission recommends continuing progress in the implementation of STIR/SHAKEN caller ID authentication technology across the voice network to reduce the number of unlawful calls, and especially calls with unlawfully spoofed caller ID information. Widespread implementation of STIR/SHAKEN will reduce the effectiveness of illegal spoofing, allowing law enforcement to identify bad actors more easily, and help voice service providers identify calls with illegally spoofed caller ID information before those calls reach consumers.

3. *Stopping Specific Scams.*—As required by the TRACED Act, the Commission has taken steps to combat specifically identified robocalling scams. In April 2020, the Commission and the Federal Trade Commission successfully pushed three gateway providers facilitating COVID-19-related scam robocalls originating overseas to stop bringing those calls into the United States within 48 hours or risk other phone companies’ being able to block all traffic from those gateway providers’ networks.<sup>61</sup> Also in April, the Commission proposed rules aimed at better protecting Americans from one-ring scam calls, which occur when a call placed to a consumer’s phone rings just once, using international toll-generating numbers that charge large fees per minute when consumers call back.<sup>62</sup> The Commission concluded this proceeding by issuing a *Report and Order* on November 30, 2020, which included a new rule to protect consumers from these scams.<sup>63</sup>

In May 2020, the Commission and the Federal Trade Commission sent additional letters to gateway providers allowing COVID-19 pandemic related scam robocalls into the United States. The letters warned that if the providers did not cut off the scam robocalls within 48 hours domestic providers would begin blocking all calls from them.<sup>64</sup> In June 2020, the Commission established a new federal advisory committee, the Hospital Robocall Protection Group (HRPG), to issue best practices on how voice service providers can better combat unlawful robocalls made to hospitals, how hospitals can better protect themselves from such calls, and how federal and

---

<sup>61</sup> See Press Release, FCC, FCC, FTC Demand Gateway Providers Cut Off Robocallers Perpetrating Coronavirus-Related Scams From United States Telephone Network (Apr. 3, 2020), <https://docs.fcc.gov/public/attachments/DOC-363522A1.pdf>; see also Press Release, FCC, FCC, FTC Demand Robocall-Enabling Service Providers Cut Off Covid-19-Related International Scammers (May 20, 2020), <https://docs.fcc.gov/public/attachments/DOC-364482A1.pdf> (noting that the previous demand letters were successful).

<sup>62</sup> *Protecting Consumers from One-Ring Scams*, CG Docket No. 20-93, Notice of Proposed Rulemaking, 35 FCC Rcd 4908 (2020).

<sup>63</sup> *Protecting Consumers from One-Ring Scams*, CG Docket No. 20-93, Notice of Proposed Rulemaking, 35 FCC Rcd 4908 (2020) (*Notice of Proposed Rulemaking*); *Protecting Consumers from One-Ring Scams*, CG Docket No. 20-93, Report and Order (released Nov. 30, 2020) (*Report and Order*).

<sup>64</sup> See Press Release, FCC, FCC, FTC Demand Robocall-Enabling Service Providers Cut Off Covid-19-Related International Scammers (May 20, 2020), <https://docs.fcc.gov/public/attachments/DOC-364482A1.pdf>.

state governments can help combat such calls.<sup>65</sup> The HRPG issued these best practices on December 14, 2020.<sup>66</sup> The TRACED Act further requires the Commission to commence a proceeding “to assess the extent to which the voluntary adoption of such best practices can be facilitated to protect hospitals and other institutions.”<sup>67</sup> This proceeding must be completed within 180 days of the HRPG’s issuance of its best practices.<sup>68</sup>

On July 27, 2020, the Enforcement Bureau selected the USTelecom Industry Traceback Group (Industry Traceback Group or ITG) as the single registered consortium to conduct private-led traceback efforts.<sup>69</sup> The Industry Traceback Group is a collaborative group comprised of providers across wireline, wireless, Voice over Internet Protocol, and cable services.<sup>70</sup> USTelecom is guided by established principles that introduce reasonable due diligence, integrity and transparency into the Traceback process.

### **Analysis and Recommendations Regarding Interconnected VoIP and Non-interconnected VoIP Service Providers that Discount High Volume, Unlawful, Short Duration Calls**

The Commission’s experience tracing back the origins of unlawful call traffic indicates that a disproportionately large number of calls originate from VoIP providers, particularly non-interconnected VoIP providers. We also have found that high-volume, rapid-fire calling is a cost-effective way to find susceptible targets. Although the Industry Traceback Group does not collect data about which robocall originators are VoIP providers,<sup>71</sup> its observations are consistent with the Commission’s.

Declining call costs over the past few decades have eliminated financial barriers to entry for would-be robocallers. Fifty years ago, domestic call rates were 25 to 50 cents per minute, and international calls cost a dollar or more per minute, with providers rounding up to the nearest minute to calculate costs.<sup>72</sup> Today, wholesale rates to U.S. mobile phones are less than a penny per minute and are accessible virtually worldwide.<sup>73</sup> Short-duration calls became popular after providers introduced six-second billing as an alternative to rounding up, as a way to become more competitive with other

---

<sup>65</sup> See Federal Communications Commission, Consumer Governmental Affairs Bureau, About the HRPG, <https://www.fcc.gov/hospital-robocall-protection-group>.

<sup>66</sup> See *Hospital Robocall Protection Group Adopts Best Practices Report on Preventing Unlawful Calls*, News Release (CGB Dec. 14, 2020).

<sup>67</sup> TRACED Act § 14(d).

<sup>68</sup> *Id.* The 180<sup>th</sup> day from issuance of HRPG best practices is June 12, 2020 (if adopted on Dec. 14, 2020). See *FCC Announces Second Meeting of the Hospital Robocall Protection Group*, Public Notice, DA-20-1417 (CGB Nov. 30, 2020).

<sup>69</sup> *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, DA 20-785 (Jul. 27, 2020) (“In this Order, the Enforcement Bureau (Bureau) selects the single consortium registered to conduct private-led traceback effort . . . the Broadband Association’s (USTelecom) Industry Traceback Group . . .”).

<sup>70</sup> *Id.*

<sup>71</sup> Affidavit of Joshua M. Bercu, Vice President of Policy and Advocacy for USTelecom – The Broadband Association at 1 (Dec. 2, 2020) (Bercu Aff.).

<sup>72</sup> Calls to and from developing nations were even more expensive. The first minute often cost more, and all calls were rounded up to the next minute.

<sup>73</sup> Bercu Aff. at 1.

providers.<sup>74</sup> This approach made short duration calls much less expensive, leading to a cottage industry of VoIP providers specializing in “dialer traffic.”<sup>75</sup> These providers compete with each other on thin margins, often with minimal staff, rented servers, online sign-ups, and virtual offices, to generate high volumes of calls.<sup>76</sup> In contrast, providers that primarily transmit conversational traffic discourage short-duration calling because it consumes network resources (thereby potentially interfering with more lucrative traffic) and is not a significant source of revenue.<sup>77</sup>

Foreign and domestic robocallers route calls through foreign VoIPs, which makes it harder for U.S. law enforcement to conduct tracebacks. However, even in these instances the Commission has successfully pushed back on VoIP providers. For example, in April and May 2020, the Commission partnered with the Federal Trade Commission to send letters to VoIP providers that were transmitting fraudulent COVID-19 robocalls that originated overseas.<sup>78</sup> Those particular calling campaigns stopped immediately after we sent the letters. We propose to continue collaborating with other federal law enforcement agencies, as well as the Industry Traceback Group and state enforcement entities, to identify the source of unlawful calls, share information, coordinate resources, and take effective measures to mitigate the unlawful calls.

Additionally, pursuant to section 6(a) of the TRACED Act, the Commission has commenced a proceeding “to determine how Commission policies regarding access to number resources, including number resources for toll-free and non-toll-free telephone numbers, could be modified, including by establishing registration and compliance obligations, and requirements that providers of voice service given access to number resources take sufficient steps to know the identity of the customers of such providers, to help reduce access to numbers by potential perpetrators of violations of [the TCPA].”<sup>79</sup> This proceeding sought comment on modifications to Commission policies that could aid in further curbing VoIP service providers that discount high volume, unlawful, short duration calls.

Finally, the Federal Trade Commission and Department of Justice, two of the Commission’s federal partners in combating illegal robocalls, have taken recent, novel actions against VoIP service providers that originated, or served as the U.S. point of entry, for large volumes of illegal calling traffic.

---

<sup>74</sup> Bercu Aff. at 1.

<sup>75</sup> “Combatting Robocall Fraud: Using Telecom Advances and Law Enforcement to Stop Scammers and Protect Seniors”, Senate Special Committee on Aging, 116<sup>th</sup> Cong., p.3 (2019) (statement of David Frankel, CEO, ZipDX LLC), [https://www.aging.senate.gov/imo/media/doc/SCA\\_Frankel\\_7\\_17\\_19.pdf](https://www.aging.senate.gov/imo/media/doc/SCA_Frankel_7_17_19.pdf) (describing “small operations – a few dozen people or perhaps just one or two” that “[b]lend in robocall traffic with their other business” to supplement their bottom line).

<sup>76</sup> *Id.*

<sup>77</sup> *Id.*

<sup>78</sup> See Press Release, FCC, FCC, FTC Demand Gateway Providers Cut Off Robocallers Perpetrating Coronavirus-Related Scams From United States Telephone Network (Apr. 3, 2020), <https://docs.fcc.gov/public/attachments/DOC-363522A1.pdf>; see also Press Release, FCC, FCC, FTC Demand Robocall-Enabling Service Providers Cut Off Covid-19-Related International Scammers (May 20, 2020), <https://docs.fcc.gov/public/attachments/DOC-364482A1.pdf>.

<sup>79</sup> TRACED Act § 6(a)(1); *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd 3241, 3292-96, paras. 123-30 (2020).

- In March, the DOJ announced a consent decree in *United States v. Kahen* that permanently bars one individual and three entities from operating as intermediate VoIP carriers conveying fraudulent robocalls into the U.S. telephone system.<sup>80</sup>
- In August, the DOJ announced a consent decree in *United States v. Palumbo* that imposed a permanent injunction barring two individuals and two companies that transmitted massive volumes of fraudulent robocalls from conveying any telephone calls into the U.S. telephone system.<sup>81</sup>
- In September, the FTC announced a stipulated order against Globex Telecom, Inc. and others in *FTC v. Educare Center Services, Inc.* that requires the VoIP company and its subsidiaries to abide by client screening and monitoring provisions.<sup>82</sup> For example, Globex and its subsidiaries cannot provide VoIP and related services to clients who pay with stored value cards or cryptocurrency, or to clients who do not have a public-facing website or social media presence. They are required to conduct a screening and review process for all potential clients, and to re-screen any existing client who is subject to a subpoena from the government or similar investigative request.
- In December, the FTC announced a stipulated order in *FTC v. Alcazar Networks Inc.* that, like the Globex order, imposes a comprehensive set of due diligence and monitoring provisions on the VoIP company.<sup>83</sup>

These actions send a strong message to VoIP providers that they may be subject to prosecution if they knowingly allow high volumes of unlawful robocalls onto their network.

### **Section 11 of the TRACED Act**

Section 11 of the TRACED Act requires the Commission to provide certain evidence about robocallers to the Attorney General, and section 11(b) requires the Commission to issue an annual report about such evidence.

The FCC is part of an interagency working group formed pursuant to the TRACED Act. The Enforcement Bureau meets regularly with Department of Justice staff and other governmental enforcement authorities to share information about calling activities that appear to violate federal laws or rules, collaborate on possible responses, and coordinate enforcement action. In addition, the Commission maintains its practice of referring unpaid forfeitures, including for robocall and spoofing violations, to the

---

<sup>80</sup> See Press Release, U.S. Department of Justice, District Court Enters Injunctions Against U.S. Based Telecommunications Carriers Facilitating Hundreds of Millions of Fraudulent Robocalls to Consumers (Mar. 27, 2020), <https://www.justice.gov/usao-edny/pr/district-court-enters-injunctions-against-us-based-telecommunications-carriers>.

<sup>81</sup> See Press Release, U.S. Department of Justice, District Court Enters Permanent Injunction Shutting Down Telecom Carriers Who Facilitated Hundreds of Millions of Fraudulent Robocalls to Consumers in The United States (Aug. 26, 2020), <https://www.justice.gov/opa/pr/district-court-enters-permanent-injunction-shutting-down-telecom-carriers-who-facilitated>.

<sup>82</sup> See Press Release, FTC, Globex Telecom and Associates Will Pay \$2.1 Million, Settling FTC's First Consumer Protection Case Against a VoIP Service Provider (Sept. 22, 2020), <https://www.ftc.gov/news-events/press-releases/2020/09/globex-telecom-associates-will-pay-21-million-settling-ftcs-first>.

<sup>83</sup> See Press Release, FTC, FTC Takes Action against Second VoIP Service Provider for Facilitating Illegal Telemarketing Robocalls (Dec. 3, 2020), <https://www.ftc.gov/news-events/press-releases/2020/12/ftc-takes-action-against-second-voip-service-provider>.

Department of Justice. As a result of our collaborative efforts we have been able to accomplish the following during the reporting period:

In March 2020, Commission staff provided evidence of a robocalling campaign transmitting false information about the coronavirus to the Consumer Protection Branch of the U.S. Department of Justice (Consumer Protection Branch). In April 2020, the Enforcement Bureau provided evidence to the Consumer Protection Branch of another large spate of robocalls attempting to scam American consumers regarding the coronavirus. The Enforcement Bureau also coordinated closely with the Federal Trade Commission and the Department of Justice regarding these robocalls. The Commission and the Federal Trade Commission sent warning letters to the service providers that were carrying the offending traffic, and the providers responded immediately by committing to stop transmitting the scam calls.<sup>84</sup>

Additionally, Enforcement Bureau staff coordinated with multiple State Attorneys General, resulting in the Commission's adopting a Notice of Apparent Liability against Rising Eagle, a Texas-based telemarketer, on June 9, 2020.<sup>85</sup> Additionally, seven State Attorneys General filed enforcement actions on the same day. We continue to meet with representatives from the FTC, DOJ, FBI, Consumer Financial Protection Bureau, Social Security Administration, Treasury Department, Postal Inspection Service, and Homeland Security on a regular basis to coordinate efforts to stop illegal robocalls.

### **Section 13 of the TRACED Act**

Section 13 of the TRACED Act requires the Commission to issue an annual report on the status of private-led efforts to trace back the origin of suspected unlawful robocalls.

#### **Private-Led Traceback Efforts**

The Commission issued rules, in accordance with Section 13 of the TRACED Act, to “establish a registration process for the registration of a single consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls.”<sup>86</sup> On July 27, 2020, the Enforcement Bureau selected the USTelecom Industry Traceback Group as the single registered consortium to conduct private-led traceback efforts.<sup>87</sup> The Industry Traceback Group is a collaborative group comprised of providers across wireline, wireless, Voice over Internet Protocol, and cable services.<sup>88</sup>

---

<sup>84</sup> See Press Release, FCC, FCC, FTC Demand Gateway Providers Cut Off Robocallers Perpetrating Coronavirus-Related Scams From United States Telephone Network (Apr. 3, 2020), <https://docs.fcc.gov/public/attachments/DOC-363522A1.pdf>; see also Press Release, FCC, FCC, FTC Demand Robocall-Enabling Service Providers Cut Off Covid-19-Related International Scammers (May 20, 2020), <https://docs.fcc.gov/public/attachments/DOC-364482A1.pdf>.

<sup>85</sup> See *John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948, 5948 (2020), <https://docs.fcc.gov/public/attachments/DOC-364824A1.pdf>.

<sup>86</sup> TRACED Act Section 13(d)(1).

<sup>87</sup> *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, DA 20-785 (Jul. 27, 2020) (“In this Order, the Enforcement Bureau (Bureau) selects the single consortium registered to conduct private-led traceback effort . . . the Broadband Association’s (USTelecom) Industry Traceback Group . . .”).

<sup>88</sup> *Id.*



USTelecom is guided by established principles that introduce reasonable due diligence, integrity and transparency into the traceback process.<sup>89</sup> The principles established by USTelecom dictate that traceback candidates will only be shared with the Industry Traceback Group if:

- 1) A credible and verifiable source is providing information regarding the traceback candidate;
- 2) The nature of the traffic associated with the traceback candidate is deemed by USTelecom staff to be fraudulent, abusive, or unlawful; and
- 3) Initiation of the traceback warrants use of the Industry Traceback Group’s valuable resources.

Traceback candidates are validated by USTelecom and the Industry Traceback Group generally through the following resources.

- **Industry Traceback Group Steering Committee Member Referrals.** Designated ITG Steering Committee Members<sup>90</sup> may identify traceback candidates. Any Steering Committee Member identifying such traceback candidates shall use good faith efforts to ensure that the traceback candidate satisfies the requirements of 47 USC 222(d)(2) (*e.g.*, calls to a Steering Committee Member’s subscribers have been identified as suspected fraud).
- **Analytics Providers.** Many analytic providers (*e.g.*, Nomorobo, YouMail) use scoring algorithms to identify suspected fraudulent traffic to their subscribers. USTelecom, on behalf of the Industry Traceback Group, may partner with such analytics providers to help identify traceback candidates.<sup>91</sup> For example, YouMail allows customers to flag voicemail messages left by robocallers. YouMail then delivers the call information and copies of the voicemails to the Industry Traceback Group for investigation.
- **Enforcement Authorities.** USTelecom seeks to cooperate with enforcement authorities at the local, state and federal level with the goal of providing such agencies with actionable leads on active Suspicious Traffic campaigns. This cooperation may also include traceback candidates identified by appropriate enforcement authorities for whom USTelecom may initiate a traceback.

---

<sup>89</sup> See USTelecom’s Industry Traceback Group, Policies and Procedures at 7 (Jan. 2020), [https://www.ustelecom.org/wp-content/uploads/2020/02/USTelecom\\_ITG-Policies-and-Procedures\\_Jan-2020.pdf](https://www.ustelecom.org/wp-content/uploads/2020/02/USTelecom_ITG-Policies-and-Procedures_Jan-2020.pdf). These Policies & Procedures were approved by the FCC. See Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), EB Docket No. 20-22, DA 20-785, para. 9 (EB rel. Jul. 27, 2020) (“Traceback Consortium Order”) (finding that the Industry Traceback Group “developed a comprehensive set of policies (referred to as the Industry Traceback Group Policies and Procedures) to document and promote consistent application of its methods”).

<sup>90</sup> Steering Committee Members implement the Policies and Procedures governing the operational aspects of the ITG and industry tracebacks. Steering Committee Members must: (1) be Cooperative Voice Service Providers that show a continuous commitment to the traceback process, including support for traceback investigations through the use of the secure traceback portal and participation in regularly scheduled ITG Member calls; (2) fully comply with the Industry Traceback Group Policies and Procedures; (3) sign a statement of intent to adopt and follow the Best Practices listed in the ITG Policies and Procedures; and (4) agree to adhere to the principles contained in the State Attorneys General Anti-Robocall Principles, <https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf>; and (5) ensure that the Industry Traceback Group Member and all of its Affiliates adhere to the State AG Anti-Robocall Principles.

<sup>91</sup> USTelecom’s Industry Traceback Group, Policies and Procedures at 12.

- **Enterprises Subject to Scams.** Businesses whose brands are being illegally used in Campaigns without authorization by the business (including, but not limited to, healthcare providers, financial institutions, utilities, technology companies) may request that USTelecom initiate a traceback on their behalf, subject to conditions and limitations on the use of the traceback results as established by the Industry Traceback Group. USTelecom may require a fee for such tracebacks.

The USTelecom Traceback team uses a secure, proprietary portal to determine the source of the traffic.<sup>92</sup> The Industry Traceback Group then notifies the terminating voice service provider(s) whose customer(s) received the suspicious traffic, which in turn may investigate the identity of the upstream voice service provider from whom it received the suspicious traffic and enter the information into the portal. After the Industry Traceback Group completes a traceback, it may refer the case to federal and state law enforcement agencies, such as the Federal Communications Commission, the Federal Trade Commission, the Department of Justice, and state Attorneys General. The referrals provide detailed information regarding the callers responsible for suspected illegal robocalls, as well as those voice service providers that actively facilitate the completion of suspected illegal calls.<sup>93</sup> The Industry Traceback Group also holds a monthly call with staff from these offices and agencies.

#### **Industry Traceback Group Coordination with the Commission**

Commission staff and the Industry Traceback Group have worked to develop an effective traceback process that assists the Commission in the continuation and evolution of the traceback process. Collaboration with private-led traceback efforts is important to unmask the identities of those entities making the illegal robocalls.

The Industry Traceback Group's tracebacks have accelerated the investigation process. A single telephone call may pass through multiple providers from the point of origin to the destination. Until very recently, each link in the chain required a separate subpoena from the FCC, FTC, or other agency to the handling provider. The length of time it takes to find the suspected violator depends on how quickly investigators can get to the origin point of the calls. The more links in the chain, the longer the investigation time. The Industry Traceback Group's efforts reduce the number of subpoenas agencies must issue to do the same work. For example, in a recent case with four links between the originating provider and the customer's provider, the Commission worked with the Industry Traceback Group to trace the origin of the call. As a result, a traceback that would have taken at least four separate subpoenas and 2 to 3 months to complete was successfully traced back in less than 24 hours.

Additionally, the FCC, FTC, and other agencies analyze the data that the Industry Traceback Group provides to identify potential enforcement targets, consider the need for new rules, declaratory rulings, or other policy actions to close loopholes and clarify obligations and restrictions.

---

<sup>92</sup> Secure Traceback Portal is an online portal managed by USTelecom to facilitate tracebacks and identification of illegal robocall Originators.

<sup>93</sup> Letter from Joshua Bercu, Vice President, US Telecom to Marlene Dortch, Secretary, Federal Communications Commission (Nov. 13, 2020), <https://ecfsapi.fcc.gov/file/11131977418160/USTelecom%20Letter%20re%20Status%20of%20Private-Led%20Traceback%20Efforts.pdf>.



The Commission provides the attached materials for this report: 1) a spreadsheet from the Industry Traceback Group listing providers and details regarding their participation in traceback efforts;<sup>94</sup> 2) a letter<sup>95</sup> from the Industry Traceback Group providing a description of private-led traceback efforts, which was filed with the Commission on November 16, 2020;<sup>96</sup> 3) a copy of the Industry Traceback Group's policies and procedures;<sup>97</sup> and 4) a copy of the Industry Traceback Group's application<sup>98</sup> to the Commission. Attachments 3 and 4, which describe the Industry Traceback Group's methodology, are referenced in the letter describing private-led traceback efforts.

---

<sup>94</sup> In accordance with the requirements of TRACED Act §§ 13(b)(2), (3), and (4), the attached spreadsheet contains the following: a list of voice service providers identified by the consortium that participated in trace back efforts, a list of each voice service provider that received a request to participate in the private led trace back efforts and refused, and the reason each voice service provider that did not participate provided. Service providers might participate in some trace back efforts and refuse to participate in others. The third tab on the spreadsheet provides more granular data for service providers that received a request in 2020 to participate in trace back efforts and declined to do so; it shows the total number of requests and the number of such requests declined.

<sup>95</sup> Letter from Joshua Bercu, Vice President, US Telecom to Marlene Dortch, Secretary, Federal Communications Commission (Nov. 13, 2020), <https://ecfsapi.fcc.gov/file/11131977418160/USTelecom%20Letter%20re%20Status%20of%20Private-Led%20Traceback%20Efforts.pdf>.

<sup>96</sup> In accordance with the requirements of TRACED Act §§ 13(b)(1) and (5), the letter provides a description of private-led efforts to trace back the origin of suspected unlawful robocalls by the registered consortium and consortium coordination with the FCC, and a description of how the FCC may use information provided by voice service providers or the registered consortium as part of private-led trace back efforts in the FCC's enforcement.

<sup>97</sup> USTelecom's Industry Traceback Group, Policies and Procedures (Jan. 2020), [https://www.ustelecom.org/wp-content/uploads/2020/02/USTelecom\\_ITG-Policies-and-Procedures\\_Jan-2020.pdf](https://www.ustelecom.org/wp-content/uploads/2020/02/USTelecom_ITG-Policies-and-Procedures_Jan-2020.pdf).

<sup>98</sup> Application of USTelecom, EB Docket No. 20-22 (filed May 21, 2020), <https://ecfsapi.fcc.gov/file/105210376506982/USTelecom-Consortium-Application.pdf>.