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, 2025

TABLE OF CONTENTS

I. INTRODUCTION

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).[1]

Section 3 of the TRACED Act requires the Commission to provide an annual report that includes data regarding certain complaints that the Commission received during the preceding five full calendar years (2020-2024), Commission enforcement actions during the preceding calendar year (2024), proposals for reducing unlawful calls, and analysis and recommendations concerning Voice over Internet Protocol (VoIP) service providers' contributions to unlawful calls.[2]

Sections 11 and 13 require the Commission to provide an annual report addressing certain Commission and private industry actions with respect to illegal robocalls as defined in 47 U.S.C. § 227(b) and (e), which prohibit unsolicited calls using an artificial or prerecorded voice message as well as calls

[1] 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.

[2] *See id.* § 3(a)(3).

made using misleading or inaccurate caller identification (caller ID) information for an improper purpose, often referred to as "robocalls."[3]

II. TELEPHONE CONSUMER PROTECTION ACT

The Telephone Consumer Protection Act (TCPA), as codified in section 227(b) of the Communications Act of 1934, as amended ("Communications Act" or "Act"), restricts calls using an automatic telephone dialing system or an artificial or prerecorded voice.[4] It prohibits calls to residential phones if the call uses an artificial or prerecorded voice message, unless the called party consents, the call is for an emergency purpose, or falls within any other enumerated exception, including any exemption adopted by a rule or order of the Commission.[5] Section 227(b) also prohibits calls made using an automatic telephone dialing system or an artificial or prerecorded voice to other types of phone lines, including calls to mobile telephone numbers, unless the called party consents, the call is for an emergency purpose, or the call falls within any other enumerated exception, including an exemption adopted by the Commission.[6] 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."[7]

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 who receive more than one telephone call within any 12-month period by or on behalf of the same entity in violation of the Commission's regulations implementing section 227(c).[8]

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 Commission's regulations implementing the TCPA, or use of any telephone facsimile machine or automatic telephone dialing system in a manner that does not comply with such standards.[9] This section prohibits the use of a computer or other electronic device to send any message via a telephone facsimile machine unless the sender 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, an identification of the entity sending the message, and the telephone number of the sending machine or the entity.[10] This section also requires that all artificial or prerecorded telephone messages shall clearly state at the beginning of the message the identity of the entity initiating the call, and, during or after the message, the telephone number or address of the entity.[11]

---

[3] *See id.* §§ 11(b), 13; *see* 47 U.S.C. § 227(b), (e).

[4] *See* 47 U.S.C. § 227(b)(1).

[5] *Id.* § 227(b)(1)(B).

[6] *Id.* § 227(b)(1)(A). The Commission has held that "calls" to mobile phones include both voice calls and text messages. *See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order, 18 FCC Rcd 14014, 14115, para. 165 (2003).

[7] *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.

[8] *See id.* § 227(c)(5); *see also* 47 CFR § 64.1200(c), (e).

[9] *See* 47 U.S.C. § 227(d)(1)(A); *see also* 47 CFR § 64.1200(a)(4)-(8), (b), (d), (e).

[10] *See* 47 U.S.C. § 227(d)(1)(B).

[11] *See id.* § 227(d)(3)(A).

III. TRUTH IN CALLER ID ACT

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 messaging service to "knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value."[12] Such practices are known as illegal "spoofing."

IV. SECTION 3 OF THE TRACED ACT

Section 3 of the TRACED Act amends the TCPA and the Truth in Caller ID Act in several respects that affect Commission enforcement. First, section 3 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).[13] 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."[14] 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.[15] 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.[16] 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) and (e) of the Communications Act.[17]

Section 3 also adds section 227(h) to the Communications Act, which requires the Commission to submit an annual report to Congress, following consultation with the Federal Trade Commission (FTC), regarding Commission enforcement of section 227(b), (c), (d), and (e) during the preceding calendar year.[18] The information section 227(h) requires in the report is provided below.[19]

A. The Number of Consumer Complaints Alleging a Violation of Section 227(b)-(e)

The chart below provides, by calendar year, from 2020 through 2024, the number of informal consumer complaints that the Commission received alleging violations of section 227(b)-(e). It is important to note that one complaint may contain several violations covered by section 227(b)-(e) and

---

[12] *Id.* § 227(e)(1); *see also* 47 CFR § 64.1604. The prohibition does not apply to "[l]awfully 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), (e)(7).

[13] *See* TRACED Act § 3(a)(1), 133 Stat. at 3274 (adding 47 U.S.C. § 227(b)(4)(A), which makes section 503(b)(5) of the Communications Act inapplicable to violations of section 227(b)). Section 3(a)(2) also amended section 227(e) to codify in statute that the Commission is not required to issue a citation pursuant to section 503(b)(5) before it proposes a monetary forfeiture under section 227(e). *See id*. § 3(a)(2), 133 Stat. at 3275 (amending 47 U.S.C. § 227(e)(5)(A)(ii)).

[14] *Id.* § 3(a)(1), 133 Stat. at 3274 (adding 47 U.S.C. § 227(b)(4)(B)). Such amounts are recoverable under section 504(a) of the Communications Act. *See* 47 U.S.C. § 504(a).

[15] TRACED Act § 3(a)(1), 133 Stat. at 3275 (adding 47 U.S.C. § 227(b)(4)(E)(ii)); *see* 47 CFR § 1.80(c)(4).

[16] TRACED Act § 3(a)(2), 133 Stat. at 3275 (amending 47 U.S.C. § 227(e)(5)(A)(iv)); *see* 47 CFR § 1.80(c)(3).

[17] *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, 4477-78, paras. 6-9 (EB 2020).

[18] TRACED Act § 3(a)(3), 133 Stat. at 3275-76 (adding 47 U.S.C. § 227(h)).

[19] *See* 47 U.S.C. § 227(h)(2).

may be counted multiple times. For example, complaints alleging spoofed caller ID prohibited under section 227(e) may also allege robocall violations under section 227(b) or Do Not Call violations under section 227(c), and thus might be counted up to three times in the following chart.

Year	227(b) Restrictions on unsolicited fax advertisements and calls made using an artificial or prerecorded voice or automated telephone dialing system	227(c) Restrictions on sales calls made to residential or wireless telephone numbers in the National Do Not Call Registry	227(d) Technical and procedural standards for communications made using facsimile machines or artificial or prerecorded voice systems	227(e) Prohibition on provision of misleading or inaccurate caller identification information with intent to defraud, cause harm, or wrongfully obtain something of value
2020	38,657	92,043	27,937	53,763
2021	46,189	97,677	28,744	57,075
2022	39,436	70,753	19,532	39,744
2023	31,042	57,917	14,715	31,594
2024	33,137	73,028	24,459	29,180

B. Citations to Enforce Section 227(d)

In 2024, the Commission did not issue any citations to enforce section 227(d).[20]

C. Notices of Apparent Liability for Forfeiture

In 2024, the Commission issued one Notice of Apparent Liability for Forfeiture to enforce section 227(b)-(e).

Steve Kramer. On May 24, 2024, the Commission issued a Notice of Apparent Liability for Forfeiture proposing a $6,000,000 fine against Steve Kramer (Kramer) for perpetrating an illegal robocall campaign targeting potential New Hampshire voters two days before the state's 2024 Democratic Presidential Primary Election in apparent violation of the Truth in Caller ID Act of 2009, which is codified at section 227(e) of the Communications Act and section 64.1604 of our rules.[21] Kramer's illegal robocalls carried a deepfake generative artificial intelligence (AI) voice message.[22] The caller ID information was inaccurate and misleading as the calls transmitted the telephone number associated with

[20] Section 3 of the TRACED Act removed 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). *See* TRACED Act § 3(a)(1), 133 Stat. at 3274 (adding 47 U.S.C. § 227(b)(4)(A)).

[21] *Steve Kramer*, Notice of Apparent Liability for Forfeiture, 39 FCC Rcd 6004, 6004, para. 1 (2024) (Kramer NAL). The Commission issued a Notice of Apparent Liability for Forfeiture to Lingo Telecom, LLC in 2024 asserting apparent violations of the Commission's rules relating to its authentication of caller ID information for the spoofed robocalls at issue in the Kramer NAL and proposing a $2,000,000 forfeiture. *See Lingo Telecom, LLC*, Notice of Apparent Liability for Forfeiture, 39 FCC Rcd 6027, 6027-28, paras. 1-3 (2024) (Lingo NAL). The Enforcement Bureau later entered into a consent decree with Lingo Telecom. *See Lingo Telecom, LLC*, Order, DA-24-790, 2024 WL 3915892 at *1 (EB Aug. 21, 2024) (Lingo Consent Decree).

[22] *See* Kramer NAL, 39 FCC Rcd at 6004, para. 1.

an unaffiliated person. Additionally, Kramer placed the calls without having received the requisite consent of the call recipients.

D. Forfeiture Orders

In 2024, the Commission issued one forfeiture order for violations of section 227(b)-(e).

Steve Kramer. On September 30, 2024, the Commission issued a Forfeiture Order imposing a penalty of $6,000,000 against Kramer for effectuating an illegal robocall campaign that targeted potential New Hampshire voters two days before the state's 2024 Democratic Presidential Primary Election (Primary Election) in violation of the Truth in Caller ID Act of 2009.[23] Kramer's illegal robocalls carried a deepfake AI voice message that imitated former U.S. President Joseph R. Biden, Jr.'s voice and encouraged potential voters not to vote in the then-upcoming Primary Election. The caller ID information was inaccurate and misleading because the calls transmitted the telephone number associated with a prominent New Hampshire political operative with whom Kramer had no association.

E. Forfeiture Penalties and Criminal Fines Collected

In 2024, neither the Commission nor the Attorney General collected forfeiture penalties or criminal fines for violations of section 227.

The Commission refers failures to pay forfeitures to the U.S. Department of Justice (DOJ) for further enforcement action. The Commission has referred forfeiture orders against the following parties for violations of section 227:

- *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.* (referred on August 10, 2018);
- *Philip Roesel, dba Wilmington Insurance Quotes,* and *Best Insurance Contracts, Inc.* (referred on December 14, 2018);
- *Affordable Enterprises of Arizona, LLC* (referred on February 23, 2021);
- *Scott Rhodes a.k.a. Scott David Rhodes, Scott D. Rhodes, Scott Platek, Scott P. Platek* (referred on March 26, 2021);
- *Kenneth Moser dba Marketing Support Systems* (referred on March 17, 2023);
- *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* (referred on June 15, 2023);
- *John M. Burkman, Jacob Alexander Wohl, J.M. Burkman & Associates LLC* (referred on July 24, 2023);
- *Sumco Panama SA, Sumco Panama USA, Virtual Telecom kft, Virtual Telecom Inc., Davis Telecom Inc., Geist Telecom LLC, Fugle Telecom LLC, Tech Direct LLC, Mobi Telecom LLC, and Posting Express Inc.* (referred on September 21, 2023);
- *Thomas Dorsher; ChariTel Inc; OnTel Inc; ScammerBlaster Inc*. (referred on November 21, 2023); and
- *Steve Kramer* (referred on December 3, 2024).[24]

---

[23] *Steve Kramer*, Forfeiture Order, FCC 24-104, 2024 WL 4432157 (Sept. 30, 2024).

[24] *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, Forfeiture Order, 33 FCC Rcd 4663 (2018); *Best Insurance Contracts, Inc., and Philip Roesel, dba Wilmington Insurance Quotes,* Forfeiture Order, 33 FCC Rcd 9204 (2018); *Affordable Enterprises of Arizona, LLC*, Forfeiture Order, 35 FCC Rcd 12142 (2020); *Scott Rhodes a.k.a. Scott David Rhodes, Scott D. Rhodes, Scott Platek, Scott P. Platek*, Forfeiture Order, 36 FCC Rcd 705 (2021); *Kenneth Moser dba Marketing Support Systems*, Forfeiture Order, 35 FCC Rcd 13415 (2020); *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*, (continued…)

F. Proposals for Reducing the Number of Unlawful Calls

The Commission has proposed and implemented a broad range of actions to combat illegal robocalls made in violation of section 227(b)-(e), with a focus on giving consumers and carriers the tools necessary to block illegal robocalls and robotexts. Below, we highlight actions the Commission took in 2024.

1. Examining New and Emerging Technologies

AI-Generated Robocall & Robotext Rules. In 2024, the Commission focused on examining both the opportunities and risks posed by rapidly advancing technologies like Artificial Intelligence (AI).

In February 2024, the Commission unanimously adopted a Declaratory Ruling confirming that the TCPA's restrictions on the use of "artificial or prerecorded voice" encompass current AI technologies that generate human voices.[25]

In August 2024, the Commission adopted a Notice of Proposed Rulemaking and Notice of Inquiry (*TCPA AI NPRM*) proposing steps to protect consumers from AI-enabled fraudulent robocalls alongside actions that clear the path for positive uses of AI, including its use to improve access to the telephone network for people with disabilities and ways AI can help consumers avoid illegal calls.[26] The *TCPA AI NPRM* also sought comment on requiring callers to specifically disclose to consumers when they are making AI-generated calls to ensure that consumers are fully apprised when granting consent to be called.

2. Further Action to Protect Consumers from Illegal Calls

Enhanced TCPA Consent Rules. The Commission also took action last year to further protect consumers from illegal calls and texts. The TCPA restricts robocalls and robotexts absent the prior express consent of the called party or a recognized exemption.[27] A consumer's right to revoke consent after deciding they no longer want robocalls or robotexts is essential to this framework. In February, the Commission adopted the *TCPA Consent Order* that (1) requires that robocallers and robotexters honor do-not-call and consent revocation requests within a reasonable time, not to exceed 10 business days from receipt, and (2) codifies that consumers can revoke consent under the TCPA through any reasonable means.[28]

Text Blocking Rule Became Effective. The Commission also continued to enlist mobile service providers in the fight against scam robotexts by announcing the September 3, 2024 effective date of a new rule requiring that mobile service providers block certain texts messages that are highly likely to be

---

Forfeiture Order, 36 FCC Rcd 6225 (2021); *John M. Burkman, Jacob Alexander Wohl, and J.M. Burkman & Associates LLC*, Forfeiture Order, 38 FCC Rcd 5529 (2023); *Sumco Panama SA, Sumco Panama USA, Virtual Telecom kft, Virtual Telecom Inc., Davis Telecom Inc., Geist Telecom LLC, Fugle Telecom LLC, Tech Direct LLC, Mobi Telecom LLC, and Posting Express Inc.*, Forfeiture Order, 38 FCC Rcd 7235 (2023); *Thomas Dorsher, ChariTel Inc., OnTel Inc., ScammerBlaster Inc.*, Forfeiture Order, 38 FCC Rcd 9139 (2023); *Steve Kramer*, Forfeiture Order, FCC 24-104, 2024 WL 4432157 (Sept. 30, 2024).

[25] *Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts*, CG Docket No. 23-362, Declaratory Ruling, 39 FCC Rcd 1783 (2024).

[26] *Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts*, CG Docket No. 23-362, Notice of Proposed Rulemaking and Notice of Inquiry, FCC 24-84, 2024 WL 3755096, at *1, para. 2 (Aug. 8, 2024) (*TCPA AI NPRM*).

[27] *See Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Report and Order and Further Notice of Proposed Rulemaking, 39 FCC Rcd 1988, 1988, para. 1 (2024) (*TCPA Consent Order*).

[28] *Id*. at 1991, para. 9.

illegal.[29] Specifically, the Commission's rules now require mobile wireless providers to block texts purporting to be from numbers on a reasonable Do-Not-Originate (DNO) list.[30] A DNO list may include only unused, unallocated, or invalid numbers, as well as numbers for which a subscriber has requested blocking. Texts purporting to be from numbers on such a list are highly likely to be illegal and this new rule is critical to combatting such scam robotexts.

Reassigned Numbers Database Utility Improved. The Commission continued to improve the utility of its Reassigned Numbers Database (RND). The Commission established the RND to prevent a consumer from getting unwanted calls intended for someone who previously held their phone number. Callers can use the RND to determine whether a telephone number may have been reassigned so they can avoid calling consumers who do not want to receive the calls. In November 2024, the Commission's Consumer and Governmental Affairs Bureau granted the RND Administrator's request to clarify that subscribers' unused queries to the RND will be added to queries purchased with a new subscription.[31] This change improves the utility of the RND for subscribers by allowing a subscriber to, within certain parameters, keep the queries it has paid for but not yet used.

Caller ID Authentication Requirements. In November 2024, the Commission adopted the *Caller ID Authentication Eighth Report and Order*, which strengthened caller ID authentication requirements by establishing rules for providers'[32] use of third parties to perform the technological act of signing calls to fulfill their authentication obligations under the Commission's rules.[33] The *Order* placed limits on the use of such third-party arrangements to ensure they do not undermine adherence to the requirements of the STIR/SHAKEN technical standards or allow providers to avoid accountability for noncompliance.[34] Specifically, it limited the third-party authentication arrangements authorized under the Commission's rules to those in which the provider with the STIR/SHAKEN implementation obligation: (1) makes all attestation level decisions, consistent with the STIR/SHAKEN technical standards, and (2) ensures that all calls are signed using its own certificate obtained from a STIR/SHAKEN Certificate Authority—not the certificate of a third party.[35] Under the new rules, utilizing a third party to sign traffic without complying with these requirements will constitute a violation of the Commission's caller ID authentication rules.[36] The *Order* further required that any provider certifying to partial or complete STIR/SHAKEN implementation in the Robocall Mitigation Database must be registered with the STIR/SHAKEN Policy Administrator, obtain its own Service Provider Code (SPC) token from the Policy Administrator, use that token to generate a certificate with a STIR/SHAKEN Certificate Authority, and authenticate all its calls with that certificate, whether directly or through a third party.[37] The *Order* also adopted recordkeeping

---

[29] *Effective Date for Text Blocking Rule Provisions Set for September 3, 2024*, CG Docket Nos. 02-278; 21-402, Public Notice, 39 FCC Rcd 2322 (CGB Mar. 13, 2024).

[30] *See* 47 CFR § 64.1200(p).

[31] *Consumer and Governmental Affairs Bureau Announces Change to Reassigned Numbers Database Usage Charge*, CG Docket No. 17-59, Public Notice, DA 24-1192, 2024 WL 4921381 (CGB Nov. 26, 2024).

[32] The general term "provider" as used in this report includes not only providers of "voice service" as defined in section 4(a)(2) of the TRACED Act, but also "intermediate providers," including "gateway providers" and "non-gateway intermediate providers," as those terms are defined in section 64.6300 of the Commission's rules.

[33] *Call Authentication Trust Anchor*, WC Docket No 17-97, Eighth Report and Order, FCC 24-120, 2024 WL 4879987, at *5, para. 14 (adopted Nov. 21, 2024). The new rules will go into effect following review and approval by the Office of Management and Budget.

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

requirements regarding third-party authentication arrangements to ensure compliance with the rules and promote accountability in the event that any such arrangement leads to abuse of the voice network.[38]

Enhanced Robocall Mitigation Requirements. Under Commission rules, all providers carrying or processing voice traffic must file certifications and robocall mitigation plans in the FCC's Robocall Mitigation Database.[39] Failure to comply with the Commission's Robocall Mitigation Database filing rules may result in the imposition of a forfeiture or removal of a deficient filing from the Database.[40] Intermediate and terminating providers are prohibited from accepting traffic directly from any providers that have not affirmatively filed or were removed from the Robocall Mitigation Database pursuant to an enforcement action.[41] The Commission has implemented a number of enhancements to these robocall mitigation requirements to ensure they serve as an effective compliance and consumer protection tool.

In August 2024, the Commission launched a proceeding that proposed and sought comment on additional steps filers should be required to take to ensure the accuracy and currentness of information submitted to the Robocall Mitigation Database.[42] Based on the resulting record, in December 2024, the Commission adopted a *Report and Order* that established new rules or amended existing rules to improve the overall quality of Robocall Mitigation Database submissions and strengthen the procedures providers must follow to submit, update, and maintain accurate filings.[43] They include requiring prompt updates when a change to a provider's information occurs; establishing a higher base forfeiture amount for providers submitting false or inaccurate information; creating a dedicated reporting portal for deficient filings; issuing substantive guidance and filer education; developing the use of a two-factor authentication log-in solution; requiring providers to recertify their Robocall Mitigation Database filings annually; and requiring providers to remit a filing fee for initial and subsequent annual submissions to cover the costs associated with processing providers' filings.[44]

---

[38] *Id.*

[39] 47 CFR § 64.6305(d)-(f).

[40] *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1903, para. 83 (2020) (*Caller ID Authentication Second Report and Order*); *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Sixth Report and Order, Fifth Report and Order, Order on Reconsideration, Order, Seventh Further Notice of Proposed Rulemaking, and Fifth Further Notice of Proposed Rulemaking, 37 FCC Rcd 6865, 6882, para. 40 (2022); *Call Authentication Trust Anchor*, WC Docket No 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2602-03, paras. 56-57 (2023) (*Caller ID Authentication Sixth Report and Order*).

[41] *See* 47 CFR § 64.6305(g)(1)-(4).

[42] *Improving the Effectiveness of the Robocall Mitigation Database*, *Amendment of Part 1 of the Commission's Rules, Concerning Practice and Procedure, Amendment of CORES Registration System*, WC Docket No. 24-213, MD Docket No. 10-234, Notice of Proposed Rulemaking, 39 FCC Rcd 92381 (2024).

[43] *Improving the Effectiveness of the Robocall Mitigation Database*, *Amendment of Part 1 of the Commission's Rules, Concerning Practice and Procedure, Amendment of CORES Registration System*, WC Docket No. 24-213, MD Docket No. 10-234, Report and Order, FCC 24-135, 2025 WL 99665, at *1, para. 3 (adopted Dec. 30, 2024). The rule establishing base forfeitures for submission of inaccurate or false information to the Robocall Mitigation Database and for failure to timely update records in the Robocall Mitigation Database will take effect 30 days after publication of the Report and Order in the Federal Register. *See id*. at *20, para. 58. Amendments to other rules adopted in the Report and Order will go into effect following publication of notices in the Federal Register. *See id*.

[44] *Id.*

3. Enforcing Obligations to Stop Illegal Robocalls

The Commission's rules place an affirmative obligation on providers to take steps to effectively mitigate illegal traffic when notified of such traffic by the Commission's Enforcement Bureau.[45] Under section 64.1200(n)(2) of the Commission's rules, providers that receive a Notification of Suspected Illegal Traffic from the Enforcement Bureau must promptly investigate the identified traffic and report back the results of their investigation and the steps taken to effectively mitigate the identified traffic or provide an explanation why the traffic was not illegal.[46] If the provider fails to do so or continues to allow substantially similar traffic onto the U.S. network, the Enforcement Bureau may issue an Initial Determination Order stating that the provider is not in compliance with the Commission's rules and give the provider a final opportunity to come into compliance.[47] If the provider does not provide an adequate response to the Initial Determination Order or continues to originate substantially similar traffic onto the U.S. network, the Enforcement Bureau may issue a Final Determination Order that directs immediate downstream providers to cease accepting the provider's traffic beginning 30 days after the release of that Order.[48]

Lingo Telecom, LLC. On February 6, 2024, the Enforcement Bureau took action to combat AI-generated illegal robocalls by issuing a Notification of Suspected Illegal Traffic to Lingo Telecom, LLC (Lingo), a provider that apparently originated spoofed[49] robocalls that used AI-generated voice cloning to spread disinformation to voters prior to New Hampshire's primary election.[50] Additionally, Lingo signed these calls with an "A-Level Attestation"[51] which signals to downstream providers in the call path that the signing provider has a direct authenticated relationship with the customer and the customer has the right to use the telephone number that appears in the caller ID field.[52] However, the number was assigned to someone other than Lingo's customer, therefore Lingo should not have provided an "A-Level Attestation."[53] The Notification of Suspected Illegal Traffic instructed Lingo to investigate the identified traffic and report its findings to the Enforcement Bureau.[54] The letter also warned that the Enforcement Bureau could initiate proceedings to direct all immediate downstream providers to cease accepting Lingo's traffic if Lingo failed to comply with the Notification of Suspected Illegal Traffic or continued to

---

[45] 47 CFR § 64.1200(n)(2).

[46] *Id*.§ 64.1200(n)(2)(i).

[47] *Id*. § 84.1200(n)(2)(ii).

[48] *See id*. § 64.1200(n)(2)(iii), (n)(3).

[49] "Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity." Fed. Commc'ns Comm'n, *Caller ID Spoofing* (last updated Nov. 13, 2024), https://www.fcc.gov/spoofing.

[50] Letter from Loyaan A. Egal, Chief, FCC Enforcement Bureau, to Alex Valencia, Chief Compliance Officer, Lingo Telecom, LLC, 2024 WL 488250, at *1 (Feb. 6, 2024), https://docs.fcc.gov/public/attachments/DOC-400264A1.pdf (Lingo Telecom Letter).

[51] Lingo Telecom Letter, at *3.

[52] *See Second Caller ID Authentication Order*, 36 FCC Rcd at 1863, para. 10; *see also* ATIS & SIP Forum, ATIS-1000074.v003, Signature-based Handling of Asserted information using toKENs (SHAKEN) at 12 (2022), https://www.sipforum.org/download/sip-forum-twg10-signature-based-handling-of-asserted-information-using-tokens-shakenpdf/?wpdmdl=2813&refresh=65c1499c3b6991707166108 (stating that, for "Full Attestation" (A-level attestation), the "signing service provider is asserting that their customer can 'legitimately' use the [telephone number] that appears as the calling party (i.e., the Caller ID).").

[53] Lingo Telecom Letter, at *3.

[54] *See id*, at *4.

originate substantially similar traffic.[55] In addition to the Notification of Suspected Illegal Traffic, the Commission issued a Notice of Apparent Liability for Forfeiture to Lingo on May 28, 2024.[56] Lingo entered into a settlement with the Enforcement Bureau on August 21, 2024.[57]

Veriwave Telco, LLC. On April 4, 2024, the Enforcement Bureau took action against apparently illegal "tax relief" robocalls by issuing a Notification of Suspected Illegal Traffic to Veriwave Telco, LLC (Veriwave) for apparently originating robocalls playing prerecorded messages pertaining to an unknown "National Tax Relief Program."[58] This robocalling campaign increased in volume in the three months immediately preceding the 2024 filing season start date.[59] This start date, and the lead up to it, may have been particularly stressful for tax filers with arrears from prior years because their 2023 tax refund could be subject to withholding by the Internal Revenue Service.[60] This robocall campaign apparently preyed upon these filers.[61] Veriwave failed to respond to the Notification of Suspected Illegal Traffic, and as a consequence the Enforcement Bureau found that Veriwave was not in compliance with section 64.1200(n)(2)(i) of the Commission's rules.[62] As a result, the Enforcement Bureau issued an Initial Determination Order on July 8, 2024.[63] The Initial Determination Order warned that failure to provide an adequate response, or continued origination or allowance onto the U.S. network of substantially similar traffic, would result in the Bureau issuing a Final Determination Order.[64]

DigitalIPvoice, Inc. On April 17, 2024, the Enforcement Bureau took action to combat apparently illegal student loan debt relief robocalls by issuing a Notification of Suspected Illegal Traffic to DigitalIPvoice, Inc. (DigitalIPvoice) for transmitting apparently illegal robocall traffic pertaining to student loan services.[65] DigitalIPvoice served as the gateway provider for multiple illegal robocalls.[66]

---

[55] *See id*, at *4-5.

[56] *See* Lingo NAL, 39 FCC Rcd at 6027.

[57] *See* Lingo Consent Decree, 2024 WL 3915892.

[58] *See* Letter from Loyaan A. Egal, Chief, FCC Enforcement Bureau, to Felix Hernandez, Compliance Officer, Veriwave Telco, LLC, 2024 WL 1526701, at *1-2 (Apr. 4, 2024), https://docs.fcc.gov/public/attachments/DOC-401632A1.pdf (Veriwave Letter).

[59] *Id.* at *1; *see* Daily Call Volume per Campaign, YouMail, Inc., https://app.sigmacomputing.com/youmailinc/workbook/ (last visited Mar. 19, 2023) (screenshot on file at EB-TCD-24-00036355); 2024 Tax Filing Season Set for January 29; IRS Continues to Make Improvements to Help Taxpayers, Internal Revenue Serv. (Jan. 8, 2024), https://www.irs.gov/newsroom/2024-tax-filing-season-set-for-january-29-irscontinues-to-make-improvements-to-helptaxpayers#:~:text=January%2029%3A%20Filing%20season%20start,Due%20date%20for%20extension%20filers (explaining the IRS began accepting 2023 tax returns on January 29, 2024).

[60] *See* Topic No. 201, The Collection Process, Internal Revenue Serv., https://www.irs.gov/taxtopics/tc201 (last visited Mar. 6, 2025) ("[A]ny future federal tax refunds or state income tax refunds that you're due may be seized and applied to your federal tax liability").

[61] Veriwave Letter, 2024 WL 1526701, at *1.

[62] *Veriwave Telco, LLC*, Initial Determination Order, DA 24-645, 2024 WL 3337668, at *1 (EB July 8, 2024), https://docs.fcc.gov/public/attachments/DA-24-645A1.pdf (Veriwave IDO).

[63] *Id.*

[64] *Id*. at *3.

[65] *See* Letter from Loyaan A. Egal, Chief, FCC Enforcement Bureau, to Stephen Matlock, CEO, DigitalIPvoice, Inc., 2024 WL 1701182 (Apr. 17, 2024), https://docs.fcc.gov/public/attachments/DOC-401896A1.pdf (DigitalIPvoice Letter).

[66] *See id.* at *1.

These calls apparently violated the Commission's rules by containing prerecorded messages directed to cell phones without an emergency purpose or prior express consent from the call recipient.[67] The letter warned that if DigitalIPvoice did not take steps to cease transmitting illegal robocall traffic, the Enforcement Bureau might ultimately direct downstream providers to block all of DigitalIPvoice's traffic.[68]

Alliant Financial. On May 20, 2024, the Enforcement Bureau took action against apparently illegal robocalls related to marketing lending services by issuing a Notification of Suspected Illegal Traffic and Additional Notification of Robocall Mitigation Database Filing Deficiencies to Alliant Financial (Alliant).[69] Alliant apparently originated calls that delivered prerecorded messages related to debt consolidation loans and claimed to be from "One Street Financial," "Main Street Financial," and "Alliant Financial."[70] The use of the latter two names risks confusion for consumers because the names are similar to the names of entirely unrelated financial entities.[71] The Notification warned that failure to comply with the obligations in section 64.1200(n) of the rules may result in the Enforcement Bureau directing downstream providers to permanently block all of Alliant's traffic.[72] The Notification of Suspected Illegal Traffic also informed Alliant that its Robocall Mitigation Database filing was deficient and outlined the steps Alliant must take to cure its deficiencies or risk removal from the Robocall Mitigation Database.[73]

Identidad Advertising Development LLC. On October 18, 2024, the Enforcement Bureau took action to combat a bank impersonation scam by issuing a Notification of Suspected Illegal Traffic to Identidad Advertising Development LLC (Identidad) for transmitting apparently illegal robocall that impersonated financial institutions.[74] These calls apparently violated the Commission's rules by containing prerecorded messages directed to cell phones without an emergency purpose or prior express consent from the call recipient.[75] The Notification of Suspected Illegal Traffic warned that if Identidad did not take steps to cease transmitting illegal robocall traffic, the Enforcement Bureau might direct downstream providers to block all of Identidad's traffic.[76]

Robocall Mitigation Database Enforcement. On December 10, 2024, the Enforcement Bureau issued an order to 2,411 providers requiring them to cure deficiencies in their Robocall Mitigation

---

[67] *Id*.

[68] *See id.* at *2-3.

[69] *See* Letter from Loyaan A. Egal, Chief, FCC Enforcement Bureau, to Mohammad Hossain, Member, Management, Alliant Financial, 2024 WL 2316149 (May 20, 2024), https://docs.fcc.gov/public/attachments/DOC-402162A1.pdf (Alliant Letter).

[70] *See id*. at *1.

[71] *See id*.

[72] *See* 47 CFR § 64.1200(n)(2); Alliant Letter at *4-6.

[73] *See id*. at *6-7.

[74] *See* Letter from Loyaan A. Egal, Chief, FCC Enforcement Bureau, to Andres Sanchez, Chief Executive Officer, Identidad Advertising Development LLC, 2024 WL 4566102 (Oct. 18, 2024), https://docs.fcc.gov/public/attachments/DOC-406703A1.pdf (Identidad Letter).

[75] *See id*. at *2.

[76] *See id*. at *3-4.

Database certifications or show cause as to why the Enforcement Bureau should not remove the certifications from the Robocall Mitigation Database.[77]

Consumer Communications Information Services Threat (C-CIST) Designation. The Enforcement Bureau adopted the C-CIST classification as a tool to identify threat actors that repeatedly use U.S. communications networks to perpetuate the most harmful, illegal schemes against consumers. The classification shines a light on the tactics, techniques, and procedures of a C-CIST's illegal operation. This allows state, federal, and international regulatory counterparts and law enforcement entities to swiftly detect and pursue appropriate action against these threat actors. The classification also arms industry stakeholders, who are the first line of defense in keeping illegal and harmful traffic off U.S. communications networks, with information that will enhance their "Know Your Customer" and "Know Your Upstream Provider" processes.[78] The C-CIST classification advances a "whole-of-government" and "public/private sector" approach to protecting consumers and businesses from harmful threat actors.

C-CIST1: Royal Tiger. On May 13, 2024, the FCC issued a Public Notice classifying a group of international providers and their managing personnel, known as "Royal Tiger", as the first C-CIST.[79] Royal Tiger is composed of a group of individuals and entities located in the United States, the United Kingdom, the United Arab Emirates, and India.[80] Royal Tiger repeatedly originated and transmitted apparently unlawful robocalls related to the impersonation of government entities, banks, and utility companies.[81] In so doing, Royal Tiger facilitated harmful and apparently unlawful calls targeting consumers in the U.S. and compromised consumer trust in the communications networks.

4. Protecting Consumers from Illegal Robocalls and Robotexts

The TCPA and STIR/SHAKEN authentication framework continue to serve as critical safeguards against illegal robocalls and robotexts. Thus, the Commission continues to focus on TCPA and call authentication-related policies.

In 2023, the Commission released the *Caller ID Authentication Sixth Report and Order* and *Direct Access Second Report and Order*, which directed the Commission's Wireline Competition Bureau to refer to the North American Numbering Council (NANC) issues regarding possible differential treatment of international cellular roaming traffic for purposes of STIR/SHAKEN caller ID authentication and possible changes to our numbering rules to prevent the misuse of numbering resources to originate

[77] *2,411 Robocall Mitigation Database Filers*, Order, DA 24-1235, 2024 WL 5090088 (EB Dec. 10, 2024), https://docs.fcc.gov/public/attachments/DA-24-1235A1.pdf.

[78] *See* 47 CFR § 64.1200(n)(4)-(5).

[79] *See* FCC Enforcement Bureau Classifies 'Royal Tiger' As A Consumer Communications Information Services Threat (C-CIST), Public Notice, 39 FCC Rcd 4587, 4587 (EB 2024), https://docs.fcc.gov/public/attachments/DA-24-388A1.pdf.

[80] *See id*.

[81] *See id*. at 4591-92.

illegal robocalls.[82] At its December 13, 2024, meeting, the NANC voted to adopt three reports providing recommendations to the Commission on these issues.[83]

On December 13, 2024, as required by the TRACED Act and section 64.6304(f) of the Commission's rules, the Wireline Competition Bureau issued a Public Notice reevaluating the two remaining STIR/SHAKEN implementation extensions granted by the Commission on the basis of undue hardship—the extension for small voice service providers originating calls via satellite using U.S. North American Numbering Plan numbers and the extension for providers that cannot obtain an SPC token—and found that they do not require revision.[84] The Bureau found that these narrow extensions remain necessary to avoid undue hardship for the limited number of providers that require them, and that retaining them does not present a significant barrier to the Commission's goal of full participation in STIR/SHAKEN.[85]

G. Analysis and Recommendations Regarding the Contribution of 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.[86] The number of VoIP providers continues to increase. The USTelecom's Industry Traceback Group (Industry Traceback Group) has identified 275 new providers in 2024 compared to 270 new providers in 2023.[87] This increase in new providers may be due to the ease with which entities can create new VoIP providers or VoIP resellers, in contrast to the financial and regulatory barriers to entry associated with establishing a new facilities-based provider.[88] Low barriers to entry and changes in technology not only contribute to the proliferation of VoIP providers, but create opportunities for threat actors to harm consumers.

Low Cost, Short Duration Calls. The Industry Traceback Group has found that high-volume, rapid-fire, calling is a cost-effective way for bad actors to find susceptible targets, although the Industry

---

[82] *See Call Authentication Trust Anchor*, WC Docket No 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2615, para. 83-85 (2023) (*Caller ID Authentication Sixth Report and Order*); *Numbering Policies for Modern Communications*, WC Docket No. 13-97, Second Report and Order and Second Further Notice of Proposed Rulemaking, 38 FCC Rcd 8951, 8986-8989 paras. 68-73 (2023) (*Direct Access Second Report and Order*); Letter from Trent Harkrader, Chief, Wireline Competition Bureau, to the Hon. Karen Charles, Chairwoman, North American Numbering Council, Call Authentication Trust Anchor Working Group (Aug. 14, 2023), https://www.fcc.gov/sites/default/files/CATA WG Referral Letter 8 14 23 PDF.pdf.

[83] *See FCC Reschedules the December Meeting of the North American Numbering Council*, WC Docket No. 23-1, Public Notice, DA 24-1006 (rel. Sept. 27, 2024); Report on the Regulatory Treatment of International Cellular Roaming Traffic, North American Number Council (2024), https://www.fcc.gov/files/cata-working-group-report-12-13-24; Report on Direct Access to Numbers by Interconnected Voice over Internet Protocol (VoIP) Providers, North American Number Council (2024), https://www.fcc.gov/files/cata-direct-access-report-12-13-24; Direct Access, North American Number Council (2024), https://www.fcc.gov/files/naowg-direct-access-report-12-13-24.

[84] *Wireline Competition Bureau Performs Required Evaluation of STIR/SHAKEN Implementation Extensions Pursuant to Section 64.6304(f) of the Commission's Rules*, WC Docket No. 17-97, Public Notice, DA 24-1252, 2024 WL 5135122, at *1 (WCB Dec. 13, 2024).

[85] *Id*.

[86] Interconnected VOIP and non-interconnected VoIP services enable real-time two-way voice communications that originate from or terminate to the user's location using internet protocol, but only interconnected VoIP service permits users generally to receive calls that originate on the public switched telephone network and terminate calls to the public switched telephone network. *See* 47 U.S.C. § 153(25) and (36); 47 CFR § 9.3.

[87] *See* Letter from Joshua M. Bercu, Executive Director, Industry Traceback Group, to Marlene Dortch, Secretary, Federal Communications Commission, at 1 (May 1, 2025) (ITG Traceback Status Letter).

[88] *See id*.

Traceback Group does not collect data about which robocall originators are VoIP providers.[89] Declining call costs over the past few decades have significantly lowered financial barriers to entry for would-be robocallers. For example, fifty years ago, long distance, 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.[90] Today, wholesale rates to U.S. mobile phones are less than a penny per minute and are accessible virtually worldwide.[91]

Short-duration calls became popular after providers introduced six-second billing, as an alternative to rounding up, to become more competitive with other providers.[92] This approach made short duration calls much less expensive, leading to a cottage industry of VoIP providers specializing in so-called "dialer traffic."[93]

Foreign and domestic robocallers route calls through foreign VoIP providers, which makes it harder for U.S. law enforcement to conduct tracebacks. These providers compete on thin margins, often with minimal staff, rented servers, online sign-ups, and virtual offices, to generate high volumes of calls.[94] In contrast, intermediate providers discourage short-duration calling because it consumes network resources (thereby potentially interfering with more lucrative traffic) and is not a significant source of revenue.[95]

Evolving Technology. Illegal robocallers evolve and there are new, concerning, trends such as voice phishing attacks that use AI-powered robocalls that mimic a real conversation.[96] Additionally, AI voice messages can be made very inexpensively and can cause significant harm to individuals and communities.[97] The TCPA authorizes the Commission to "prescribe technical and procedural standards for systems that are used to transmit any artificial or prerecorded voice message via telephone."[98] In the *TCPA AI NPRM* the Commission stated that "the legislative history of the TCPA reveals that Congress

[89] Affidavit of Joshua M. Bercu, Vice President of Policy and Advocacy for USTelecom – The Broadband Association at 1 (Dec. 2, 2020) (Bercu Aff.).

[90] *Id.*

[91] *Id*.

[92] *Id*.

[93] *Id*. The Commission has found that access stimulation or "traffic pumping" occurs when a local exchange carrier with high switched access rates enters into an arrangement with a provider of high call volume operations, such as chat lines, adult entertainment calls, and "free" conference calls, to stimulate the local exchange carrier's terminating access minutes. The local exchange carrier will typically share the inflated revenues with the high volume provider. *See, e.g.*, *Updating the Intercarrier Compensation Regime to Eliminate Access Arbitrage*, Notice of Proposed Rulemaking, 33 FCC Rcd 5466, 5467, para. 2 (2018).

[94] Bercu Aff., at 1; *see also Combatting Robocall Fraud: Using Telecom Advances and Law Enforcement to Stop Scammers and Protect Seniors: Hearing Before the S. Special Committee on Aging*, 116th Cong. 3 (2019) (statement of David Frankel, CEO, ZipDX LLC), 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).

[95] Bercu Aff., *supra* note 89, at 1.

[96] *Id*.

[97] Kramer NAL, *supra* note 21 at 6008, para. 9 (Kramer paid an individual $150 to make the deepfake voice message used for the calls).

[98] *TCPA AI NPRM*, 2024 WL 3755096, at *2, para. 6; *see also* 47 U.S.C. § 227(d)(3).

anticipated that the Commission would have the flexibility to apply the TCPA's privacy protections from illegal robocalls to future technologies as well as existing technologies."[99]

The Commission also acknowledges that the practices of illegal robocallers can negatively affect legitimate callers. A call from legitimate businesses may be ignored or marked as spam if a recipient suspects it is an illegal robocall. As a result, consumers may miss essential notifications, appointment reminders, or security alerts.[100] As the Commission continues to explore the implications of AI with respect to robocalls, the Commission supports protecting businesses' ability to innovate and implement positive uses of the technology.[101]

V. SECTION 11 OF THE TRACED ACT

Section 11(a) of the TRACED Act requires the Chief of the Enforcement Bureau to provide evidence that suggests a willful, knowing, and repeated robocall violation with an intent to defraud, cause harm, or wrongfully obtain anything of value to the Attorney General.[102] As used in Section 11(a), "robocall violation" refers narrowly to calls that violate 47 U.S.C. § 227(b) or (e) of the Act, principally, calls to a cell phones or residential lines using an artificial or prerecorded voice without the consent of the recipient or other applicable exemption, calls to cell phones using an automatic telephone dialing system, or calls that are illegally spoofed.[103] Section 11(b) requires the Commission to annually publish on its website and submit to Congress a report that provides (1) the number of instances during the preceding year in which the Commission has provided such evidence to the Attorney General; and (2) a general summary of the types of violations to which such evidence relates.[104]

In 2024, the Commission coordinated with the DOJ on eight matters involving callers who impersonated banks, political operatives, charities, commercial retailers, the Social Security Administration, and local law enforcement in apparent violation of 47 U.S.C. § 227(b) and/or 47 U.S.C. § 227(e). The Commission also coordinated with the DOJ to staff the Federal Bureau of Investigation (FBI) National Election Command Post during election week to assist with any robocall-related interference matters.

The Commission also met on a regular basis with representatives from the FTC, DOJ, FBI, the Consumer Financial Protection Bureau, the Social Security Administration, the Department of the Treasury, the Postal Inspection Service, the Department of Education, the Department of Homeland Security, and the Department of Veterans Affairs to coordinate efforts to stop illegal robocalls.

---

[99] *See TCPA AI NPRM*, 2024 WL 3755096, at *2, para. 6; *see also* See 137 Cong. Rec. S18784 (1991) (statement of Sen. Hollings) ("The FCC is given the flexibility to consider what rules should apply to future technologies as well as existing technologies"). The Commission's interpretation of the TCPA has accounted for new technologies that fell within its scope. *See, e.g.*, Rules and Regulations Implementing the Telephone Consumer Protection Act, Westfax Inc. Petition for Consideration and Clarification, CG Docket Nos. 02-278, 05-338, Declaratory Ruling, 30 FCC Rcd 8620 (2015) (confirming that an "efax," a document sent as a conventional fax but then converted and delivered as an electronic email attachment was covered by the TCPA's consumer protections from unwanted junk faxes).

[100] *See* Trestle, *The Consequences of Robocalls and Scam Calls for Major Industries* (July 22, 2024), https://trestleiq.com/consequences-of-robocalls/.

[101] *TCPA AI NPRM*, 2024 WL 3755096, at *1, para. 2 ("[we] propose steps to protect consumers from the abuse of AI in robocalls alongside actions that clear the path for positive uses of AI[.]"); *TCPA AI NPRM*, 2024 WL 3755096, Statement of Commissioner Brendan Carr ("When it comes to the broader regulation of AI . . . we need to make sure we continue to support U.S. innovation and leadership.").

[102] TRACED Act § 11(a), 133 Stat. at 3285 (codified at 47 U.S.C. § 227b-2(a)).

[103] *See id.* § 11(d), 133 Stat. at 3286 (codified at 47 U.S.C. § 227b-2(d)); 47 U.S.C. § 227(b), (e).

[104] *Id.* § 11(b), 133 Stat. at 3285 (codified at 47 U.S.C. § 227b-2(b)).

VI. SECTION 13 OF THE TRACED ACT

Section 13(a) of the TRACED Act requires the Commission to annually publish on its website and submit to Congress a report on the status of private-led efforts to trace back the origin of suspected unlawful robocalls.[105] On March 27, 2025, the Enforcement Bureau issued a Public Notice pursuant to section 13 of the TRACED Act, seeking information about traceback efforts in 2024.[106] The Public Notice requested "comment on private-led efforts to trace back the origin of suspected unlawful robocalls and to issue an annual report on the status of such efforts and the participation of voice service providers in such efforts."[107] On May 1, 2025, the Industry Traceback Group filed a letter on the status of private-led tracebacks for 2024.[108]

A. Private-Led Traceback Efforts

The Commission issued rules, in accordance with section 13(d) 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."[109] In 2024, the Commission conducted the annual selection process to select the registered consortium to conduct private-led traceback efforts in accordance with section 13(d) of the TRACED Act and section 64.1203 of the Commission's rules. No entities submitted letters of intent in response to the Enforcement Bureau's Public Notice. As a result, the Industry Traceback Group continues to serve as the registered consortium.[110] The Industry Traceback Group is a collaborative group composed of providers across wireline, wireless, VoIP, and cable services.[111]

The Industry Traceback Group is guided by established principles that introduce reasonable due diligence, integrity, and transparency into the traceback process.[112] These principles dictate that tracebacks will be conducted only if:

1) A credible and verifiable source is providing information regarding the traceback candidate;

---

[105] TRACED Act § 13(a), 133 Stat. at 3287.

[106] *See Enforcement Bureau Requests Information On The Status Of Private-Led Traceback Efforts Of Suspected Unlawful Robocalls*, EB Docket 20-195, Public Notice, 2025 WL 947266 (EB 2025).

[107] *Id*.

[108] *See* ITG Traceback Status Letter.

[109] TRACED Act § 13(d)(1), 133 Stat. at 3287-88.

[110] The Bureau issued a public notice on April 26, 2024 requesting interested consortia to provide letters of intent to conduct private-led traceback effort in accordance with the Commission's rules. *See Enforcement Bureau Requests Letters of Intent to Become the Registered Industry Consortium for Tracebacks*, EB Docket No. 20-22, Public Notice, 39 FCC Rcd 2929 (EB. 2024); 47 CFR § 64.1203(a). No letters of intent were submitted in response to that public notice. As the current registered consortium, the Industry Traceback Group was not required to file a letter of intent. *See* 47 CFR § 64.1203(c).

[111] *See* Industry Traceback Group, About Us, https://tracebacks.org/about/ (last visited Mar. 7, 2025) ("Adherence to the Policies and Procedures fosters cooperation by a broad range of supportive industry participants, including incumbent local exchange carriers, competitive local exchange carriers, wireless carriers, cable and VoIP providers, and wholesale providers . . .").

[112] *See* Industry Traceback Group, Policies and Procedures at 10 (Apr. 2022), https://tracebacks.org/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr-2022.pdf (*Industry Traceback Group Policies and Procedures*).

2) The nature of the traffic associated with the traceback candidate is deemed by Industry Traceback Group staff to be fraudulent, abusive, or unlawful; and

3) Initiation of the traceback warrants use of the Industry Traceback Group's valuable resources.[113]

The following parties generally initiate traceback requests, although the Industry Traceback Group may also independently initiate tracebacks that satisfy the above referenced criteria:[114]

- **Industry Traceback Group Steering Committee Member Referrals.** Designated Industry Traceback Group Steering Committee Members[115] 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 U.S.C. § 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. The Industry Traceback Group may partner with such analytics providers to help identify traceback candidates.[116] 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.** The Industry Traceback Group 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 the Industry Traceback Group may initiate a traceback.
- **Organizations Subject to Abusive Calling and Scams.** Public and private organizations, including businesses whose brands are being illegally used in robocall campaigns without authorization by the business (including, but not limited to, healthcare providers, financial institutions, utilities, and technology companies), may request that the Industry Traceback Group 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 Policies and Procedures*.[117] The Industry Traceback Group may require a fee for such tracebacks.

---

[113] *Industry Traceback Group Policies and Procedures* at 10.

[114] *See id*. at 10-11.

[115] Steering Committee Members implement the *Industry Traceback Group Policies and Procedures* governing the operational aspects of 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 Industry Traceback Group 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 Industry Traceback Group Policies and Procedures; (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. *See Industry Traceback Group Policies and Procedures* at 6.

[116] *See Industry Traceback Group Policies and Procedures* at 10.

[117] *See id*. at 9.

The Industry Traceback Group uses a secure, proprietary portal to determine the source of the traffic.[118] The Industry Traceback Group notifies the terminating voice service provider whose customer received the suspicious traffic, which then investigates the identity of the upstream provider from whom it received the suspicious traffic and enters the information into the portal. In turn, each provider in the call path determines the identity of the upstream provider from whom it received the suspicious traffic and enters the information into the portal.[119] The process continues until the originating voice service provider is identified or a dead end is reached.[120] After the Industry Traceback Group completes a traceback, it may refer the case to federal and state agencies that have relevant law or regulatory enforcement responsibilities, such as the Commission, the FTC, DOJ, and state attorneys general. The referrals provide detailed information regarding the callers responsible for suspected illegal robocalls, as well as those providers that actively facilitate the completion of suspected illegal calls.[121] The Industry Traceback Group also holds a monthly call with representatives from these offices and agencies.

B. Industry Traceback Group Coordination with the Commission

The Commission 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. Early in the traceback process, each link in the chain required a separate subpoena from the Commission, FTC, or other agency to the handling provider. However, the process has become much more efficient and effective, as (1) our traceback skills evolved, and (2) the Commission has updated its regulations—such as the rule that took effect in May 2021, requiring providers to respond to traceback requests in a timely manner, and the recent rule amendment requiring providers to respond to traceback requests within 24 hours, which took effect on January 8, 2024.[122] 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 greatly improve the ability of the Commission and other law enforcement entities to pursue investigations quickly.

The Commission uses the information that the Industry Traceback Group provides to support findings of violations of its rules. For instance, Notifications of Suspected Illegal Traffic cite tracebacks (and sometimes the provider's responses to such tracebacks) as evidence that the provider is apparently originating or transmitting illegal traffic and as examples of the traffic that the provider must no longer transmit.

During the past four years, the Industry Traceback Group has expanded the scope of its traceback efforts as threat actors have developed new tactics. For example, the Industry Traceback Group has started tracing back an increasing number of apparently spoofed, live, calls.[123] This has resulted in a greater number of tracebacks overall, and a smaller percentage of suspected unlawful robocalls compared to the prior year. For example, in 2024, the Industry Traceback Group initiated 3,606 tracebacks of

---

[118] The Secure Traceback Portal is an online portal managed by the Industry Traceback Group to facilitate tracebacks and identification of illegal robocall originators. *See id.* at 5.

[119] *See Industry Traceback Group Policies and Procedures*, *supra* note 112, at 8.

[120] *See id*.

[121] *See Industry Traceback Group Policies and Procedures*, *supra* note 112, at 12.

[122] *See* 47 CFR § 64.1200(n)(1).

[123] ITG Traceback Status Letter, *supra* note 87, at 1.

suspected unlawful robocalls—131 fewer tracebacks than were conducted in 2023.[124] During the same time, the number of live calls increased from 607 in 2023 to 1,408 in 2024. Also in 2024, the Industry Traceback Group identified 714 U.S.-based and foreign providers in tracebacks.[125] Of those 714 providers, 275 had not previously been identified by the Industry Traceback Group.[126] Further, in 2024, 69% of completed tracebacks resulted in an originating provider warning or terminating the caller.[127] This is a decrease from 84% in 2023.[128]

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;[129] (2) a May 1, 2025 letter from the Industry Traceback Group providing a description of private-led traceback efforts;[130] and (3) a copy of the Industry Traceback Group's policies and procedures.[131]

[124] *See id*.

[125] *Id.*

[126] *Id.*

[127] *Id.*

[128] *See id*.

[129] In accordance with the requirements of TRACED Act § 13(b)(2), (3), and (4), the attached spreadsheet contains the following information for the date range of January 1, 2024 to December 31, 2024: (1) a list of voice service providers identified by the consortium that participated in traceback efforts; (2) a list of each voice service provider that received a request to participate in the private-led traceback efforts and refused; and (3) the reason, if any, each voice service provider that did not participate provided. Service providers might participate in some traceback efforts and refuse to participate in others. The third tab on the spreadsheet provides more granular data for service providers that received a request to participate in traceback efforts and declined to do so.

[130] *See* ITG Traceback Status Letter, *supra* note 87. 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 traceback efforts in the FCC's enforcement.

[131] *Industry Traceback Group Policies and Procedures*, *supra* note 112.