Legal and Regulatory Considerations for Robocalling and Telemarketing Activities
Last Updated May 2023

This document is intended to provide a helpful guide to some of the laws, regulations, and expectations that apply to calling activities. This information does not constitute legal advice, is not exhaustive and does not include state-specific rules. Individuals and/or companies therefore are strongly advised to consult with their own counsel. Given the rapid regulatory and enforcement developments in the robocall space, information contained in this document may be quickly superseded and/or outdated.

Since January 2020, there has been a rapid and unprecedented increase in federal statutory and regulatory frameworks impacting individuals and/or companies engaged in any aspect of telemarketing or robocalling activities. These comprehensive legal frameworks have been accompanied with a noticeable escalation in robocalling enforcement activities at both the federal and state level. Collectively, these new legal constructs and enforcement activities have thrust new obligations on, and expectations from, a broad range of entities engaged in telemarketing and/or robocalling activities, including the companies originating such calls, voice providers in every part of the call path (*e.g.*, originating, transit), as well as entities that assist and/or facilitate the delivery of suspected illegal robocalls.

Increased Regulation of Robocalling Activities.
Individuals and/or companies engaged in any aspect of telemarketing or robocalling activities have long been subject to a host of statutory and regulatory frameworks governing such calls. When the Pallone Thune TRACED Act (the "TRACED Act") was signed into law on December 30, 2019, it marked one of the most significant updates to telecommunications laws since passage of the Telecommunications Act of 1996 (the "96 Act"), nearly three decades earlier. In stark contrast to the broad scope of the 96 Act, the TRACED Act initiated sweeping regulatory reforms narrowly targeting entities engaged in telemarketing and/or robocalling activities.

The TRACED Act commenced an unprecedented level of regulatory activity at the Federal Communications Commission (FCC) which has resulted in numerous rulemaking proceedings, dozens of orders, and new regulatory constructs. The FCC continues to implement further revisions to its already sizable stable of regulations governing robocalls, and the Federal Trade Commission (FTC) and state Attorneys General continue to aggressively enforce regulations under the Telemarketing Sales Rule (TSR) and other applicable laws.

Mounting Enforcement Actions Targeting Telemarketers, Robocallers, and Voice Providers.
A broad range of parties engaged in these activities could also be subject to increasing federal and state enforcement actions. Federal enforcement efforts have generally been spearheaded by the FCC, the FTC, as well as the Department of Justice (DOJ). Multiple state Attorneys General have also substantially increased their enforcement activities, including through the formation of a nationwide Anti-Robocall Litigation Task Force of 50 Attorneys General to investigate and take legal action against the telecommunications companies responsible for illegal robocalls. The two largest fines in the FCC's history were related to enforcement actions related to robocalls.

These increased enforcement efforts are also part of a larger trend, where federal and state agencies have clearly opened a new front on the fight against illegal robocalls by closely coordinating joint enforcement initiatives. For example, the FCC has announced Memoranda of Understanding between state robocall investigators and the FCC's Enforcement Bureau in 44 states and the District of Columbia. Examples of these federal and state enforcement initiatives are provided in Appendix A.

Federal and state enforcement authorities have held a broad range of voice providers accountable for illegal robocalling and telemarketing activities enabled through their networks in some circumstances, including when they originate, transit, or otherwise have "assisted and facilitated" in the generation of, such calls. These actions, which have increased substantially in recent years, have ranged from citations and fines to business shutdowns and – in some instances – imprisonment.

The following summary is provided as a general and concise overview of relevant laws and associated enforcement actions.

Table of Contents

Summary of Relevant Statutes and Regulations

1. Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)

Regulated and Enforced by: FCC
Relevant Citations: 47 USC § 227; 47 CFR § 64.1200

In an effort to comprehensively address the growing problem of illegal robocalls, Congress overwhelmingly passed the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act), which was signed into law in late 2019. The TRACED Act implemented an expansive regulatory framework that governs the activities of a broad range of stakeholders in the voice ecosystem. Among other things, the TRACED Act required the FCC to: (1) implement regulations compelling providers of "voice service" (a broadly defined term)[1] to develop and deploy call authentication technologies; (2) establish regulatory frameworks permitting blocking of suspected illegal robocalls; and (3) formalize the traceback process through the designation of a single traceback consortium. Since passage of the TRACED Act in late 2019, the FCC has undertaken an unprecedented and ongoing regulatory initiative to implement its various requirements. These efforts have resulted in numerous and affirmative regulatory obligations that have been placed on a broad range of providers, some of which are highlighted below.

a. Examples of TRACED Act Regulations

i. TRACED Act Regulations Governing Providers of Voice Service

(1) ***A Voice Provider May Have All its Traffic Blocked.*** In certain instances, the FCC may *authorize* downstream, domestic voice service providers to block the traffic of a suspected upstream bad-actor provider. A voice service provider may block calls from an upstream voice service provider that, when notified that it is carrying bad traffic by the FCC, fails to effectively mitigate such traffic or fails to implement effective measures to prevent new and renewing customers from using its network to originate illegal calls. In such instances, the downstream voice service provider blocking the traffic is protected from liability under a regulatory safe harbor. 47 CFR § 64.1200(k)(4).

(2) ***A Voice Provider Shall Have All its Traffic Blocked.*** In other instances,

[1] The FCC's implementing regulations under the TRACED Act, define "voice service" as "(1) any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan or any successor to the North American Numbering Plan adopted by the Commission under section 251(e)(1) of the Communications Act of 1934, as amended; and (2) Includes transmissions from a telephone facsimile machine, computer, or other device to a telephone facsimile machine." 47 CFR § 64.1600(r).

the FCC may *require* downstream, domestic voice service providers to block the traffic of a suspected upstream bad-actor provider. A voice service provider is required to block calls from an upstream voice service provider that, when notified that it is carrying bad traffic by the FCC, fails to effectively mitigate such traffic or fails to implement effective measures to prevent new and renewing customers from using its network to originate illegal calls. 47 CFR § 64.1200(n)(2).

(3) ***Affirmative Obligation to Respond to Tracebacks Within 24 Hours.*** All providers of voice service – including originating, transit, and gateway providers – must respond to all traceback requests from the Commission, civil law enforcement, criminal law enforcement, or the industry traceback consortium within 24-hours (FCC 23-37, ¶¶ 21 – 28) (*rule section pending regulatory approval*).

(4) ***Affirmative Obligation to Mitigate Robocalls.*** Take steps to effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission through its Enforcement Bureau. 47 CFR 64.1200(n)(2).

(5) ***Affirmative Obligation to Mitigate Origination of Illegal Robocalls.*** Take affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic. 47 CFR 64.1200(n)(3).

(6) ***Requirement to Register in the FCC's Robocall Mitigation Database (RMD).*** All providers of voice service must register in the FCC's RMD and file a robocall mitigation plan, regardless of their deployment status of the STIR/SHAKEN call authentication standard. (FCC 23-18, ¶¶ 28 - 52) (*rule section pending regulatory approval*). In a 2022 Public Notice, the FCC recently declined to extend the STIR/SHAKEN deployment deadline of June 30, 2023, for a broad range of providers, including small providers.

(7) ***Obligation to Submit a Robocall Mitigation Plan.*** All providers of service – regardless of their STIR/SHAKEN deployment status – must submit contact information for a person responsible for addressing robocall mitigation-related issues and describe in detail their robocall mitigation practices in the FCC's RMD (FCC 23-18, ¶¶ 28 - 52) (*rule section pending regulatory approval*)

(8) ***Prohibition on Accepting Voice Traffic from Providers Not Listed in the RMD.*** Intermediate providers and voice service providers are prohibited

from accepting calls directly from a domestic voice service provider unless that voice service provider's filing appears in the Robocall Mitigation Database. 47 CFR § 64.6305(e)(1).

(9) ***Prohibition on Accepting Voice Traffic from Foreign Providers Not Listed in the RMD.*** Beginning April 11, 2023, Voice Service Providers are prohibited from accepting calls directly from a foreign voice service provider or foreign intermediate provider that uses North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States, unless that foreign provider's filing appears in the Robocall Mitigation Database. 47 CFR § 64.6305(e)(2).

(10) ***Prohibition on Accepting Voice Traffic from Gateway Providers Not Listed in the RMD***. Beginning April 11, 2023, intermediate providers and voice service providers are prohibited from accepting calls directly from a gateway provider unless that gateway provider's filing appears in the FCC's RMD. 47 CFR § 64.6305(e)(3). Further, all downstream providers will be prohibited from accepting any traffic from a Non-Gateway Intermediate Provider not listed in the RMD, either because the provider did not file, or their certification was removed as part of an FCC enforcement action. 47 CFR § 64.6305(g)(3) (*rule section pending regulatory approval*).

ii. TRACED Act Regulations Governing Gateway Providers

(1) ***Obligation to Deploy and Certify to STIR/SHAKEN Authentication.*** Gateway providers must certify to the status of STIR/SHAKEN implementation and robocall mitigation on their networks in the RMD by January 11, 2023 (47 CFR § 64.6305(d)(1)) and must deploy the STIR/SHAKEN standard by June 30, 2023. 47 CFR § 64.6302(c).

(2) ***Obligation to Submit a Robocall Mitigation Plan.*** Gateway providers must submit contact information for a person responsible for addressing robocall mitigation-related issues and describe in detail their robocall mitigation practices in the FCC's RMD. 47 CFR § 64.6305(b).

(3) ***24-Hour Traceback Response Obligation.*** Gateway providers must respond to traceback requests from the Commission, law enforcement, and the industry traceback consortium within 24 hours, and must cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls. 47 CFR § 64.6305(b).

(4) ***Mandatory Blocking Obligation.*** Gateway providers that are properly notified by the FCC, must block identified illegal traffic and any substantially similar traffic on an ongoing basis (unless its investigation determines that the traffic is not illegal) when it receives actual written notice of such traffic by the FCC through its Enforcement Bureau. 47 CFR § 64.1200(n)(5). A gateway provider's failure to block such traffic, could result in *all* of its traffic being blocked by its downstream providers. 47 CFR § 64.1200(n)(6).

(5) ***Mandatory DNO Blocking Obligation.*** As of December 12, 2022, gateway providers are required to block calls based on any reasonable Do Not Originate list. 47 CFR § 64.1200(o).

(6) ***Obligation to 'Know Your Upstream' Provider.*** As of January 16, 2023, gateway providers are required to take reasonable and effective steps to ensure that the immediate upstream foreign provider is not using the gateway provider to carry or process a high volume of illegal traffic onto the U.S. network. 47 CFR §64.1200(n)(4).

(7) ***General Obligation to Mitigate Illegal Robocalls.*** Gateway providers are required to meet a general obligation to mitigate illegal robocalls regardless of whether they have fully implemented STIR/SHAKEN on the IP portions of their network. 47 CFR § 64.6305(b)(2).

iii. TRACED Act Regulations Governing Intermediate Providers

(1) ***Obligation to Accept Calls Only from Foreign Provider Registered in the RMD.*** Beginning April 11, 2023, Intermediate Providers shall accept calls directly from a foreign voice service provider or foreign Intermediate Provider that use NANP resources that pertain to the US in the caller ID field to send voice traffic to residential or business subscribers in the US, only if that foreign provider's filing appears in the RMD. 47 CFR § 64.6305(e)(2).

(2) ***Obligation to Accept Calls Only from Providers Registered in the RMD.*** Beginning April 11, 2023, Intermediate Providers shall accept calls directly from a Gateway Provider only if their filings appears in the RMD. 47 CFR § 64.6305(e)(3). Intermediate Providers shall accept calls directly from a domestic voice service provider only if that provider's filing appears in the RMD. 47 CFR § 64.6305(e)(1).

(3) ***Obligation to 'Know Your Upstream' Provider.*** Intermediate Providers are required to take reasonable and effective steps to ensure that the immediate upstream provider is not using it to carry or process a high

volume of illegal traffic (FCC 23-37, ¶¶ 49 – 51) (*rule section pending regulatory approval*).

(4) ***24-Hour Traceback Response Obligation.*** All Intermediate Providers must respond to traceback requests from the Commission, law enforcement, and the industry traceback consortium within 24 hours, and must cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls (FCC 23-37, ¶¶ 21 – 28) (*rule section pending regulatory approval*).

(5) ***Affirmative Obligation to Mitigate Robocalls*.** All Intermediate Providers must take steps to effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission through its Enforcement Bureau (FCC 23-18, ¶¶ 28 – 35) (*rule section pending regulatory approval*).

(6) ***Affirmative Obligation to Respond and Provide Accurate Information***. All Intermediate Providers are required to respond and provide accurate information to the FCC regarding the source from which they received illegal traffic (FCC 23-37, ¶ 36) (*rule section pending regulatory approval*).

iv. TRACED Act Regulations Governing Non-Gateway Intermediate Providers

(1) ***Obligation to Deploy the STIR/SHAKEN Standard in Certain Instances.*** A Non-Gateway Intermediate Provider must, not later than December 31, 2023, authenticate caller identification information for all calls it receives directly from an originating provider and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, unless that Non-Gateway Intermediate Provider is subject to an applicable extension. (FCC 23-18, ¶¶ 15 – 20) (*rule section pending regulatory approval*).

(2) ***Obligation to Register in the RMD and Submit a Robocall Mitigation Plan.*** All Non-Gateway Intermediate Providers must affirmatively register in the RMD and submit a robocall mitigation plan. A Non-Gateway Intermediate Provider's robocall mitigation plan must include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and in a timely manner to all traceback requests. (FCC 23-18, ¶¶ 28 – 52) (*rule section pending regulatory approval*).

b. Special Considerations for Voice Providers Originating Telemarketing Calls Based on Lead Generation.

i. ***Role of Know Your Customer.*** The FCC's Enforcement Bureau Chief recently emphasized the central role of 'Know Your Customer' (KYC) principles for providers of voice service when he stated that such principles "should be at the forefront of all communications service providers' business practices."[2] Although KYC principles are not expressly delineated under the FCC's rules, the agency has initiated at least one enforcement action against a voice provider based on its originating calls on behalf of its customer who was in apparent violation of the TCPA's consent requirements.[3]

ii. ***Obligation to Mitigate Origination of Robocalls Through "Reasonable Steps."*** The FCC's rules require that *all* providers of voice service mitigate the origination of illegal robocalls from their networks under a general "reasonable steps" standard. 47 CFR § 64.6305(a)(2). The FCC has stated that a voice provider's compliance with this obligation will be deemed insufficient if it "knowingly or through negligence" originates unlawful robocall campaigns.[4]

iii. ***Sufficiency of Consent.*** The FCC's mitigation obligation referenced above is closely related to issues regarding sufficiency of consent. (*See*, Sections 2.b(i) – (vii), below) Because voice providers must take "reasonable steps" to mitigate illegal robocalls "originating" from their networks, they should ensure that their originating customers do not generate traffic with telltale characteristics of illegal robocalls. (47 CFR § 64.6305(a)(2)) These characteristics include, but are not limited to, high call volume, a high number of complaints (*e.g.*, from consumers, downstream providers, government agencies, etc.), and high call volumes to numbers on the DNC.

iv. ***Potential Exposure Under the TSR.*** Given the broad range of FCC regulatory obligations for providers of voice service, failure to satisfy those obligations could potentially expose providers to separate liability under the TSR. Where a voice provider has failed to take "reasonable steps" to mitigate illegal robocall traffic,[5] or "knowingly or through negligence" originates such traffic,[6] the FTC and/or state

---

[2] *See*, FCC Press Release, *FCC Takes on Mortgage Scam Robocall Campaign Targeting Homeowners*, January 24, 2023.

[3] *See*, Public Notice, *Robocall Enforcement Notice to all U.S.-Based Voice Service Providers*, DA 23-65, p. 4 (January 24, 2023) (stating that the calls in question "independently appear to violate the Telephone Consumer Protection Act of 1991 (TCPA) and the Commission's rules, as they are prerecorded voice telemarketing messages sent to consumers without consent.").

[4] *Call Authentication Trust Anchor*, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18, ¶ 31 (rel. Mar. 17, 2023) ("*Gateway Order*").

[5] *Call Authentication Trust Anchor*, Second Report and Order, FCC 20-136, 36 FCC Rcd 1859, ¶ 76 (rel. Oct. 1, 2020).

[6] *Id.*, ¶ 78.

Attorneys General have targeted such providers for "assisting and facilitating" illegal robocalls under the TSR,[7] including for activities related to "lead generation."[8] The FTC has also recently clarified that the TSR requires the seller to obtain permission directly from the recipient of the call, and that the seller cannot rely on third-parties to obtain permission. The FTC has further clarified that a seller cannot place calls with prerecorded messages to consumers whose information the seller obtained from third-parties.

[7] *See e.g.*, *Complaint for Permanent Injunction, Damages and Other Equitable Relief*, State of Ohio v. Aaron Michael Jones, *et. al.*, S.D. Ohio, Case: 2:22-cv-02700-ALM-KAJ (July 7, 2022); *see also*, *See e.g.*, *State of North Carolina v. Articul8 LLC, et. al.*, Complaint for Injunctive Relief and Civil Penalties, S.D. Ohio, Case 1:22-cv-00058, ¶¶ 58 - 64 (Filed January 25, 2022) ("*Articul8 Complaint*") (stating that when call traffic includes characteristics such as high call volumes, use of multiple TNs/snowshoeing, high number of unanswered calls, the provider originating the traffic "knew, or consciously avoided knowing, that [it] regularly routed across its network millions of short-duration and unanswered calls with average Calls-Per-ANI in the single digits.").

[8] *Id.*, at p. 4, ¶¶ 34, 40, 91, 108.

2. Telephone Consumer Protection Act of 1991 (TCPA)
Regulated and Enforced by: FCC, State Attorneys General, Private Lawsuits
Relevant Citations: 47 USC § 227; 47 CFR § 64.1200

In an effort to address a growing number of telephone marketing calls, Congress enacted the Telephone Consumer Protection Act (TCPA) in 1991. The TCPA restricts the use of automatic telephone dialing systems (*i.e.*, "autodialers") and artificial or prerecorded voice messages in the making of telephone calls. In 1992, the FCC adopted rules to implement the TCPA, including the requirement that entities making telephone solicitations institute procedures for maintaining company-specific do-not-call lists.

In 2003, the FCC revised its TCPA rules to establish, in coordination with the Federal Trade Commission (FTC), a national Do-Not-Call registry. The national registry is nationwide in scope, covers all telemarketers (with the exception of certain nonprofit organizations), and applies to both interstate and intrastate calls. The registry went into effect on October 1, 2003, and is administered by the FTC. The FCC's website includes additional information and guidance on its regulation and enforcement of the TCPA.

a. Examples of TCPA Regulations Governing Telemarketers

i. ***Restrictions on Use of ATDS and Prerecorded Messages*.** Absent prior express consent, any person (*e.g.*, a telemarketer) is prohibited from using an autodialer *or* an artificial or prerecorded voice message to deliver a call to any emergency telephone line, or any telephone number assigned to a paging service or wireless phone. 47 CFR §64.1200(a)(1). Telemarketing calls to any residential or cellular line using an artificial or prerecorded voice to deliver a message generally require prior express *written* consent. 47 CFR § 64.1200(a)(2)-(3).

Courts generally have found that consent must be from the party that is actually called, even if a prior number holder provided valid consent. The FCC established the Reassigned Number Database to help callers avoid making calls to numbers that have been reassigned.

ii. ***Telemarketing Call Connection Requirements*.** No person or entity may disconnect an unanswered telemarketing call prior to at least 15 seconds or four (4) rings. 47 CFR § 64.1200(a)(6).

iii. ***Prerecorded Message Requirements*.** All artificial or prerecorded voice telephone messages must contain several elements, including:

(1) **Identification of the Calling Party.** A statement at the beginning of the message, that clearly identities the business, individual, or other entity that is responsible for initiating the call. If a business is responsible for initiating the call, the name under which the entity is registered to conduct business with the State

Corporation Commission (or comparable regulatory authority) must be stated. 47 CFR § 64.1200(b)(1).

(2) **Disclosure of the Business Number.** During or after the message, the calling party must clearly state the telephone number (other than that of the autodialer or prerecorded message player that placed the call) of such business, other entity, or individual. The telephone number provided may not be a 900 number or any other number for which charges exceed local or long-distance transmission charges. 47 CFR § 64.1200(b)(2).

(3) **Providing Called Parties with Opt-Out Mechanisms.** If the telemarketing call includes or introduces an advertisement or constitutes telemarketing to a residential or cellular line, the telemarketer must provide an automated, interactive opt-out mechanism. When the message is left on an answering machine or a voice mail service, it must include a toll-free number that enables the called person to call back and connect directly to the automated, interacted opt-out mechanism. 47 CFR § 64.1200(b)(3).

iv. ***Timing Restrictions on Telephone Solicitations*.** No person or entity may initiate a telephone solicitation to any residential telephone subscriber before the hour of 8 a.m. or after 9 p.m. (local time at the called party's location). 47 CFR § 64.1200(c)(1).

v. ***Do Not Call Restrictions on Telephone Solicitations*.** No person or entity may initiate a telephone solicitation to a residential telephone subscriber who has registered his or her telephone number on the national do-not-call registry of persons who do not wish to receive telephone solicitations that is maintained by the Federal Government, unless certain conditions are met. 47 CFR § 64.1200(c)(2).

b. Special Considerations for Telemarketing Based on Lead Generation.

The FCC and other enforcement agencies have brought enforcement actions against callers and originating Voice Service Providers for high-volume telemarketing calls where the caller purports to have consent. Consent often is not valid and may even be fraudulently manufactured at times, including by unaffiliated third parties that sell falsely obtained leads.

Parties engaged in telemarketing based on lead generation face a high evidentiary threshold – and potentially significant liability – based on existing legal precedent. To have prior express written consent, a seller must obtain a written agreement from the consumer that clearly authorizes the seller to make autodialed or prerecorded advertising or telemarketing calls. 47 CFR § 64.1200(f)(9). In obtaining that written agreement, the seller must provide the consumer with "clear and conspicuous notice" that he or she is agreeing to receive telemarketing calls. 47 CFR § 64.1200(f)(9)(i); 47 CFR § 64.1200(f)(3). The

FCC has noted that "it is well-settled that '[c]allers contending that they have the prior express consent to make prerecorded voice or autodialed calls to cell phones or other mobile service numbers have the burden of proof to show that they obtained such consent.'"[9]

Evidence that consent may be flawed includes:

i. ***High Call Volumes Are an Indicator of Lack of Consent.*** In the telecommunications industry, high volumes of short-duration and unanswered calls are among the analytics recognized as indicative of unwanted, fraudulent, or illegal call traffic. The FCC previously concluded call blocking programs using reasonable analytics could identify unwanted calls through a variety of characteristics, including "large bursts of calls in a short timeframe; low average call duration; low call completion ratios; invalid numbers placing a large volume of calls."[10] Federal and state enforcers have relied on such data to bring enforcement actions. The FCC recently issued a Notice of Apparent Liability (NAL) targeting perpetrators of illegal auto-warranty robocalls, noting that the entities in question used equipment and services designed to "[deliver a] message to hundreds of thousands of businesses or households per hour" and "call an unlimited amount of individuals per day."[11] The FCC emphasized that the perpetrators of the calls were in some instances able to "generate more than 15,000 calls at once."[12]

ii. ***High Call Volumes to Telephone Numbers on DNC Demonstrates Lack of Consent.*** High volumes of calls to phone numbers on the FCC's Do Not Call (DNC) Registry can also be a strong indicator of fraudulent and illegal call traffic.[13] In a recent Notice of Apparent Liability (NAL), the agency determined that a high percentage of calls to numbers on the DNC was a sufficient indicator that the targets of the FCC action "apparently intentionally violated, or at least ignored, the TCPA's consent requirements.[14] Further, the FCC recently justified a $225 million

[9] FCC 22-99, ¶ 45. *See also Dialing Services, LLC*, Forfeiture Order, 32 FCC Rcd 6192, 6200, ¶ 23 (2017) (quoting *Dialing Services, LLC*, Citation and Order, 28 FCC Rcd 1840, 1842-43, ¶ 7 (2013)); *see also Request of ACA International for Clarification and Declaratory Ruling*, Declaratory Ruling, 23 FCC Rcd 559, 565, ¶ 10 (2008) (stating that "the burden will be on [the caller] to show it obtained the necessary prior express consent").

[10] *Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51, 34 FCC Rcd 4876, ¶ 35 (rel. June 7, 2019) ("*2019 Declaratory Ruling*").

[11] *In the Matter of Sumco Panama, et. al*, Notice of Apparent Liability for Forfeiture, FCC 22-99, ¶ 41 (Dec. 23, 2022) ("*Auto Warranty NAL*").

[12] *Id.*, ¶ 43.

[13] *Articul8 Complaint*, ¶ 59.

[14] *Auto Warranty NAL*, ¶ 47.

forfeiture due in part to the agency's view that the defendant "acted deliberately to transmit calls to consumers who had listed their numbers on the National [DNC] Registry."[15] In a separate action directing all voice providers to mitigate robocall traffic associated with two entities, the FCC noted that a "significant portion" of the calls "were placed to consumers who had their phones actively listed on the DNC registry."[16] More recently, the complaint filed by the DOJ on behalf of the FTC noted that the VoIP provider was "transmitting robocalls for which the sellers and telemarketers could not demonstrate . . . that they had obtained an express agreement from each call's recipient to receive pre-recorded calls from that seller or telemarketer," and that those factors should have "made clear" that it was "transmitting calls to phone numbers on the National DNC Registry belonging to consumers for whom the seller or telemarketer could not demonstrate having obtained an express agreement or having an established business relationship."[17]

iii. ***Calls Hitting Honeypots and Other Data Sources.*** Federal and state enforcement agencies are increasingly relying on the use of honeypots to identify illegal robocalls. A "honeypot" is a set of thousands of telephone numbers that are unassigned to consumers or businesses, that answers and traps incoming calls by capturing caller IDs and voice recordings. Since 2012, the FTC has employed honeypots in its fight against robocallers,[18] and more recently the agency has relied on honeypots set up by voice providers in issuing several Cease and Desist letters.[19]

iv. ***Claimed Consent is Not Germane to Website Source.*** Recent federal and state enforcement actions have focused on the use of "opt in" websites by defendants to place robocalls to consumers, including to numbers on the DNC registry.

---

[15] *In the Matter of John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; et. al*, Forfeiture Order, FCC 21-35, 36 FCC Rcd 6225, ¶ 63 (Mar. 18, 2021).

[16] Public Notice, *Robocall Enforcement Notice to All U.S.-Based Voice Service Providers*, DA 23-65, p. 4 (January 24, 2023).

[17] *See United States of America v. XCast Labs, Inc.*, Complaint for Permanent Injunction, Civil Penalties, and Other Relief and Demand For Jury Trial, United States District Court Central District of California, No. 23-cv-03646, ¶ 42 (May 12, 2023).

[18] *See* Prepared Statement of The Federal Trade Commission, Before the United States Senate Special Committee on Aging, *Combatting Illegal Robocalls: Initiatives to End the Epidemic*, n. 53 (June 10, 2015) (stating that the FTC launched its robocall honeypot in 2012, and utilizes it to "collect evidence against robocallers and facilitate a more rapid robocall response."). *See also* Congressional Research Service Report, Protecting Consumers and Businesses from Fraudulent Robocalls, n. 50 (October 4, 2018) (available at: https://crsreports.congress.gov/product/pdf/R/R45070/12).

[19] *See, e.g.*, Cease and Desist Demand Letter, from the Federal Trade Commission to Range, Inc., also d/b/a Range Telecom (April 4, 2023); *see also*, Cease and Desist Demand Letter, from the Federal Trade Commission to Business Telecommunications Services, Inc. (March 17, 2023); Cease and Desist Demand Letter, from the Federal Trade Commission to Every1 Telecom (March 17, 2023).

However, as federal and state enforcers have noted, many of these websites are often entirely unrelated to the topic of the telemarketing call, often did not contain any language relevant to the telemarketing call, and purportedly would simultaneously give consent to many entities.[20] Further, a recent FCC rulemaking has proposed amending the agency's TCPA consent requirements to require that consent be considered granted only to callers logically and topically associated with the website that solicits consent and whose names are clearly disclosed on the same web page.[21]

v. ***'Snowshoeing' Can be an Indicia of Fraudulent Calls.*** 'Snowshoeing' describes the practice of spreading voice traffic over many outbound phone numbers to avoid filtering and blocking on the termination end of the call. In other words, instead of using a single number to make millions of calls, illegal robocallers will use hundreds of thousands of validly assigned phone numbers a single time to make the same number of calls. In a recent enforcement action, the FCC concluded that the use of 500,000 phone numbers to make the calls appear to consumers as if they were originating locally, violated its rules. The FCC concluded that the matching originating and destination numbers supported a finding of deliberately transmitting misleading caller ID similar to so-called "neighbor spoofing."[22] State Attorneys General have also cited to this practice as an indicia of illegal robocalling.[23]

[20] *State of Ohio, ex rel, Attorney General Dave Yost v. Aaron Michal Jones, et al.*, Complaint for Permanent Injunction, Damages and Other Equitable Relieve, United States District Court Southern District of Ohio, No. 2:22-CV-2700, ¶ 68 (July 7, 2022) ("*Auto Warranty Complaint*").

[21] *In the Matter of Targeting and Eliminating Unlawful Text Messages*, Report and Order and Further Notice of Proposed Rulemaking, FCC 23-21, ¶ 61 (rel. Mar. 17, 2023).

[22] Order, *In the Matter of FCC Enforcement Bureau Warns All U.S.-Based Voice Service Providers To Avoid Or Cease Carriage Of Auto Warranty Robocall Traffic From Cox/Jones/Sumco Panama Operation*, DA 22-784, ¶ 8 (rel. Jul. 21, 2022) ("*Auto Warranty Blocking Order*").

[23] *See e.g.*, *Articul8 Complaint*, ¶¶ 60 - 64 (stating that "when a provider's call traffic consists of high volumes of short duration *and* unanswered calls and also shows an average Calls-Per-ANI in the single digits, this is a strong indication that the call traffic is nefarious.") (emphasis in original).

3. Truth in Caller ID Act of 2009
Relevant Citations: 47 USC § 227(e); 47 CFR §§ 64.1600, 64.1604
Regulated and Enforced by: FCC

In order to address the growing problem of caller ID spoofing done for fraudulent or harmful purposes, Congress enacted the Truth in Caller ID Act in 2009. The Act makes it "unlawful for any person within the United States, in connection with any telecommunications service or IP- enabled voice service, to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value."

Under the Truth in Caller ID Act, FCC rules prohibit anyone from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm or wrongly obtain anything of value. Anyone who is illegally spoofing can face penalties of up to $10,000 for each violation. Although there are legitimate, legal uses for spoofing, the FCC has aggressively enforced the Truth in Caller ID Act on many occasions. In fact, one of the largest fines in the FCC's history was based on violations of the Truth in Caller ID Act.[24] Further, the FCC has recently interpreted its Truth in Caller ID Act rules to apply in instances even where the telemarketer has been assigned actual telephone numbers (*i.e.*, spoofing of telephone numbers is not necessarily required).[25] The FCC's website includes additional information and guidance on its regulation and enforcement of the Truth in Caller ID Act.

a. Examples of Truth in Caller ID Requirements

i. ***Telemarketers Must Transmit Caller ID Information*.** Any person or entity that engages in telemarketing must transmit caller identification information. 47 CFR § 64.1601(a).

ii. ***Telemarketers are Prohibited from Transmitting Inaccurate or Misleading Caller ID Information*.** No person or entity in the United States, nor any person or entity outside the United States if the recipient is within the United States, may with the intent to defraud, cause harm, or wrongfully obtain anything of value, knowingly cause, directly, or indirectly, any caller identification service to

[24] Forfeiture Order, *John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; et al.*, FCC 21-35 (Mar. 2021).

[25] Notice of Apparent Liability, Aaron Michael Jones, *et al*, FCC 22-784, ¶ 8 (Jul. 2022) (stating that calls made during the robocall campaigns "displayed inaccurate or misleading caller identification, with an apparent intent to defraud, cause harm, or wrongfully obtain something of value, in violation of the Truth in Caller ID Act and section 64.1604 of the Commission's rules," and that the entities involved "purchased nearly 500,000 numbers from at least 229 area codes in November and December 2020 apparently to make the calls appear to consumers as if they were originating locally." The FCC concluded that the "matching originating and destination numbers in consumer complaints support a finding of deliberately transmitting misleading caller ID similar to so-called 'neighbor spoofing.'").

transmit or display misleading or inaccurate caller identification information in connection with any voice service or text messaging service. 47 CFR § 64.1604(a).

iii. ***Use of Assigned Numbers May Still Violate Truth in Caller ID Act.*** In a recent enforcement action, the FCC concluded that the use of 500,000 phone numbers to make the calls appear to consumers as if they were originating locally, violated its rules. The FCC concluded that the matching originating and destination numbers supported a finding of deliberately transmitting misleading caller ID similar to so-called "neighbor spoofing."[26]

[26] *Auto Warranty Blocking Order*, ¶ 8.

4. The Telemarketing Sales Rule (TSR)
Relevant Citations: 15 U.S.C. §§ 6101-6108; 15 U.S.C. §§ 6151-6155; 16 CFR § 310
Regulated and Enforced by: FTC, State Attorneys General

The FTC's Telemarketing Sales Rule (TSR) has been in effect since December 31, 1995. The underlying statutory authority for the TSR is the Telemarketing and Consumer Fraud and Abuse Prevention Act (TCFPA), which gave the FTC and state attorneys general law enforcement tools to combat telemarketing fraud.

Companies violating the TSR could be subject to fines of up to $11,000 per violation. The FTC defines telemarketing as any "plan, program, or campaign . . . to induce the purchase of goods or services or a charitable contribution" involving more than one interstate telephone call. With some important exceptions, any businesses or individuals that take part in "telemarketing" must comply with the TSR. This is true whether, as "telemarketers," they initiate or receive phone calls to or from consumers, or as "sellers," they provide, offer to provide, or arrange to provide goods or services to consumers in exchange for payment.

The FTC also has focused on Voice over Internet Protocol (VoIP) providers. Specifically, the FTC has sent letters to VoIP service providers warning them that "assisting and facilitating" illegal telemarketing or robocalls could constitute a violation of the TSR and noting that the FTC successfully sued a VoIP service provider for TSR violations.

The do not call provisions of the TSR cover any plan, program or campaign to sell goods or services through interstate phone calls. This includes calls by telemarketers who solicit consumers, often on behalf of third-party sellers. It also includes sellers who provide, offer to provide, or arrange to provide goods or services to consumers in return for some type of payment as part of a telemarketing transaction.

The TSR requires telemarketers to make specific disclosures of material information; prohibits misrepresentations; sets limits on the times telemarketers may call consumers; prohibits calls to a consumer who has asked not to be called again; and sets payment restrictions for the sale of certain goods and services.

The FTC's website includes additional information and guidance on its regulation and enforcement of the TSR.

a. Examples of TSR Regulations Governing Sellers, Telemarketers, Other Parties.

i. ***Prohibition on Deceptive Telemarketing Acts or Practices.*** Sellers and telemarketers are prohibited from:

- Failing to disclose the total costs to purchase, receive, or use, and the quantity of, any goods or services that are the subject of the sales offer. 16 CFR §

310.3(a)(1)(i).

- Failing to disclose all material costs or conditions to receive or redeem a prize that is the subject of the prize promotion. 16 CFR § 310.3(a)(1)(v).

ii. ***Persons May Not Assist or Facilitate Deceptive Telemarketing Practices*.** It is a deceptive telemarketing act or practice and a violation of this Rule for a person to provide substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in any act or practice that violates the TSR. 16 CFR § 310.3(b).

iii. ***Prohibition on Abusive Telemarketing Acts or Practices*.** Sellers and Telemarketers are prohibited from:

- Causing any telephone to ring, or engaging any person in telephone conversation, repeatedly or continuously with intent to annoy, abuse, or harass any person at the called number. 16 CFR § 310.4(b)(1)(i).

- Initiating any outbound telephone call to a person when that person previously has stated that he or she does not wish to receive an outbound telephone call made by or on behalf of the seller whose goods or services are being offered or made on behalf of the charitable organization for which a charitable contribution is being solicited. 16 CFR § 310.4(b)(1)(iii)(A).

- Abandoning any outbound telephone call. An outbound telephone call is "abandoned" under this section if a person answers it and the telemarketer does not connect the call to a sales representative within two (2) seconds of the person's completed greeting. 16 CFR § 310.4(b)(1)(iv).

5. The Wire Fraud Statute

Relevant Citations: 18 USC §§ 1343, 1349; 47 U.S.C § 503(b)(1)(D)
Enforced by: DOJ and FCC

Under Section 1343 of Title 18, Crimes and Criminal Procedure of the U.S. Code, there are two elements to a wire fraud violation: (1) a scheme to defraud, and (2) the use of an interstate wire or radio communication to further the scheme. The statute addresses fraudulent conduct that may also come within the reach of other federal criminal and/or civil statutes and includes both civil and criminal provisions. In the criminal context, crimes are punishable by imprisonment for not more than 20 years; for not more than 30 years, if the victim is a financial institution or the offense is committed in the context of major disaster or emergency. The DOJ's Criminal Resource Manual details the elements of wire fraud.

Section 503(b)(1)(D) of the Communications Act also allows the FCC to pursue a forfeiture penalty against any person who has violated the federal wire fraud statute.

6. State AG Guidance to Voice Service Providers, Including VoIP Providers

In August of 2019, 51 attorneys general and 12 telecommunications providers agreed to certain principles to fight illegal robocalls. The purpose of this effort was to help protect phone users from illegal robocalls and to make it easier for attorneys general to investigate and prosecute violators.

The principles address the robocall problem in two main ways: prevention and enforcement. For voice service providers, including VoIP providers, the principles recommend that such companies:

1. Monitor their networks for robocall traffic;
2. Know who their customers are so bad actors can be identified and investigated;
3. Investigate and take action against suspicious callers – including notifying law enforcement and state attorneys general;
4. Work with law enforcement, including state attorneys general, to trace the origins of illegal robocalls; and
5. Require telephone companies with which they contract to cooperate in traceback investigations.

A copy of the principles can be accessed here.

7. Sampling of Robocall Enforcement Actions

a. Examples of Cease and Desist Letters Sent to Voice Providers.

Since as early as 2020, the FTC and FCC have sent cease and desist (C&D) letters to over multiple VoIP and gateway providers instructing them to cease and desist in the transmission of suspected illegal robocall traffic. With the passage of the TRACED Act in late 2019, the FCC has substantially increased the pace and volume of such C&D letters, and has also leveraged new regulatory mechanisms enabling the agency to permit – and in some cases require – downstream voice providers to block voice traffic from the identified providers.

i. 2020.

At the height of the COVID-19 pandemic, the FCC and FTC sent joint letters to five VoIP providers advising each company that, if after 48 hours of receipt of the letter, the companies continued to route or transmit harmful robocall traffic, the FCC would authorize other U.S. voice providers to block all their calls. Each company was also advised that the FCC would "take any other steps as needed to prevent further transmission of unlawful calls" and would also "evaluate whether further action is appropriate in connection with your activity."

- FCC/FTC C&D Letter to RSCom.
- FCC/FTC C&D Letter to PTGi International Carrier Services, Inc.
- FCC/FTC C&D Letter to Intelepeer Cloud Communications LLC.
- FCC/FTC C&D Letter to Connexum.
- FCC/FTC C&D Letter to VoIP Terminator.

ii. 2021

Starting in 2021, and subsequent to passage of the TRACED Act, the FCC increased the pace of C&D letters and issued more than a dozen C&D letters to VoIP providers.

- **March 18, 2021**
  - FCC C&D Letter to Yodel Tech.
  - FCC C&D Letter to Third Rock.
  - FCC C&D Letter to Stratics Networks.
  - FCC C&D Letter to RSCom.
  - FCC C&D Letter to IDT Corp.
  - FCC C&D Letter to Icon Global.

- **April 13, 2021**
  - FCC C&D Letter to Tellza.
  - FCC C&D Letter to R Squared.

- **May 18, 2021**
  - FCC C&D Letter to Prestige DR VoIP.
  - FCC C&D Letter to VaulTel Solutions.

- **October 21, 2021**
  - FCC C&D Letter to PZ/Illum Telecommunication.

- FCC C&D Letter to Primo Dialler.
- FCC C&D Letter to Duratel.

iii. 2022

Starting in 2022, the FCC's C&D letters began leveraging the agency's newly established regulatory framework to authorize – and in some cases require – downstream providers to block all traffic from voice providers transiting illegal traffic. During this timeframe, the FCC mandated the blocking of traffic from certain voice providers associated with fraudulent auto warranty and student loan debt robocalls.

- **February 10, 2022**
  - FCC C&D Letter to Great Choice Telecom.
  - FCC C&D Letter to TCA VoIP.

- **March 22, 2022**
  - FCC C&D Letter to Airespring .
  - FCC C&D Letter to Hello Hello Miami.
  - FCC C&D Letter to thinQ.

- **July 7, 2022** – The FCC's C&D letters addressed fraudulent robocall traffic associated with auto warranty robocalls. It reflected the first instance in which the FCC subsequently directed all domestic voice providers to block voice traffic from certain of the identified VoIP providers.
  - FCC C&D Letter to Call Pipe.
  - FCC C&D Letter to Fugle Telecom.
  - FCC C&D Letter to Geist Telecom.
  - FCC C&D Letter to Global Lynks.
  - FCC C&D Letter to Mobi Telecom.
  - FCC C&D Letter to SD Telecom.
  - FCC C&D Letter to SipKonnect.
  - FCC C&D Letter to Virtual Telecom.
    - July 7, 2022: FCC Public Notice *authorizing* downstream providers to block voice traffic from C&D letter recipients.
    - July 21, 2022: FCC Order *requiring* downstream providers to block voice traffic from C&D letter recipients.

- **November 10, 2022** – The FCC's C&D letter addressed fraudulent robocall traffic associated with student loan robocalls. It was the second instance in which the FCC subsequently directed all domestic voice providers to block voice traffic from the VoIP provider identified in the initial C&D letter.
  - FCC C&D Letter to Urth Access.
    - November 10, 2022: FCC Public Notice *authorizing* downstream providers to block voice traffic from the C&D letter recipient.
    - December 8, 2022: FCC Order *requiring* downstream providers to block voice traffic from C&D letter recipients.

iv. 2023

- The FCC started off 2023, by issuing three C&D letters to voice providers. They included two

C&D letters to SIPphony and Vultik on January 11, 2023, and a subsequent letter to Twilio on January 24, 2023.

b. Examples of FCC Enforcement Actions Delisting Providers from the RMD

i. On October 3, 2022, the FCC Robocall Response Team announced Enforcement Orders against seven voice service providers listed in the agency's RMD. The enforcement actions were described as "first-of-their-kind," and represented the latest example of the FCC cracking down on illegal robocallers and voice service providers routing their traffic. The Enforcement Orders directed the providers to respond to the FCC's Enforcement Bureau by October 18, 2022 to "demonstrate why the Enforcement Bureau ... should not remove" them from the RMD. The FCC' Enforcement Bureau subsequently issued an Order immediately delisting one of those providers (Global UC) from the FCC's RMD. An accompanying Public Notice directed all intermediate providers and terminating voice service providers to "cease accepting traffic from Global UC within two (2) business days." Although the Public Notice states that the other six providers updated their certifications by the October 18 deadline, it stated that the Enforcement Bureau continues "to assess the sufficiency of the robocall mitigation plans provided by these six companies."

c. Examples of FCC Enforcement Actions Under TCPA

i. *Aaron Michael Jones, et al*. The FCC unanimously adopted a Notice of Apparent Liability (NAL) for Forfeiture of nearly $300 million targeting the so-called Cox/Jones Enterprise that was responsible for more than 5 billion auto warranty robocalls. In addition to violations of the TCPA, the FCC also alleged violations of the Truth in Caller ID Act. The proposed $300 million forfeiture is the largest in the FCC's history. Prior to the issuance of the NAL, and through a series of coordinated announcements, the Ohio Attorney General announced the filing of a lawsuit identifying 22 defendants involved in the calls. In a separate but related initiative, the FCC issued eight cease and desist letters to VoIP providers, including some of the VoIP defendants in the Ohio AG's case.

ii. *Kenneth Moser dba Marketing Support Systems*. The FCC's Enforcement Bureau issued a citation to Kenneth Moser after concluding that he sent more than 11,000 prerecorded voice messages to wireless phones, without consent, in violation of the TCPA. The Enforcement Bureau found that Moser also violated the TCPA's requirement that prerecorded messages include the phone number and identity of the entity responsible for initiating the call. The citation accompanied a Notice of Apparent Liability proposing a $10 million fine against Moser for actions related to the calls.

iii. *Call-Em-All, LLC*. The FCC's Enforcement Bureau issued a citation to Call-Em-All, LLC for violating the TCPA's rules that prohibit making calls to cell phones using autodialers or artificial or prerecorded messages absent an emergency purpose or prior express consent. The citation noted that if the company failed to comply with the TCPA, it could be liable for significant penalties, including fines of up to $16,000 per call.

iv. *Yakim Jordan a/k/a Manasseh Jordan, et. al*. The FCC's Enforcement Bureau issued a citation to Yakim Jordan (a/k/a Manasseh Jordan and Manasseh Jordan Ministries) for violating the TCPA's rules that prohibit making calls to cell phones using autodialers or artificial or prerecorded messages absent an emergency purpose or prior express consent.

d. Examples of FCC Enforcement Actions Under the Truth in Caller ID Act

i. *John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group, LLC, et al*. The FCC proposed a $225 million fine against Texas-based health insurance telemarketers for allegedly making approximately 1 billion illegally spoofed robocalls in apparent violation of the Truth in Caller ID Act. This is the largest proposed fine in the FCC's 86-year history. Rising Eagle allegedly made approximately 1 billion spoofed robocalls across the country during the first four-and-a-half months of 2019 on behalf of clients that sell short-term, limited-duration health insurance plans. Mr. Spiller admitted that he knowingly called consumers on the FTC's Do Not Call list as he believed that it was more profitable to target these consumers. He also admitted that he made millions of calls per day, and that he was using spoofed numbers.

ii. *Thomas Dorsher; ChariTel Inc; OnTel Inc; and ScammerBlaster Inc*. In July, 2022, the FCC approved a Notice of Apparent Liability for Forfeiture (NAL) against Thomas Dorsher, ChariTel Inc, OnTel Inc, and ScammerBlaster Inc for allegedly engaging in a toll-free robocall traffic pumping scheme, in violation of the TCPA, that used revenue generated from the scheme to fund dangerous telephony denial of service attacks. The $116 million proposed fine represents the FCC's first TCPA enforcement action targeting entities engaged in a toll-free traffic-pumping scheme, signaling the agency's willingness to take action against unlawful robocalls made to businesses.

iii. *Adrian Abramovich, Marketing Strategy Leaders, Inc. et. al*. The FCC fined Adrian Abramovich $120 million for malicious spoofing that was part of a massive robocalling operation aimed at selling timeshares and other travel packages. The caller ID spoofing operation made almost 100 million spoofed robocalls over three months, in violation of the Truth in Caller ID Act.

iv. *Philip Roesel, dba Wilmington Insurance Quotes, et. al*. The FCC fined telemarketer Philip Roesel and his companies more than $82 million for illegal caller ID spoofing. Using spoofed caller ID information, Roesel made more than 21 million robocalls to market health insurance, and to generate leads for such sales, in violation of the Truth in Caller ID Act.

e. Examples of FTC Enforcement Actions Under the TSR

i. *Project Point of No Entry*. In April 2023, the FTC announced the implementation of Project Point of No Entry (PoNE), targeting "point of entry" or "gateway" VoIP service providers and warning they must work to keep illegal robocalls out of the country. Through Project PoNE, the FTC: 1) identifies point of entry VoIP service providers that are routing or transmitting illegal call traffic; 2) demands they stop doing so and warns their conduct may violate the TSR; and then 3) monitors them to pursue recalcitrant providers, including by opening law enforcement investigations and filing lawsuits when appropriate. The FTC can seek civil penalties and court injunctions to stop TSR violations and can also seek money to refund to consumers who were defrauded via illegal telemarketing calls. The FTC coordinates directly with the agency's federal and state partners, which support the program and pursue their own actions to fight illegal telemarketing robocalls. The FTC has made publicly available the letters it issued to twenty-four VoIP providers between May 10, 2022, and April 4, 2023.

ii. *FTC v. Educare Centre Services; Globex Telecom, Inc*. The FTC and Ohio Attorney General entered into a $2.1 million settlement with VoIP service provider Globex and its associates, settling allegations that Globex provided a company called Educare with the means to deliver illegal robocalls pitching bogus credit card interest rate reduction services to consumers. The FTC and Ohio Attorney General argued that Globex assisted and facilitated Educare's underlying scheme, in violation of the TSR and Ohio law. The settlement was the FTC's first consumer protection case against a VoIP provider.

iii. *FTC v. James Christiano*. In June 2018, the FTC filed a complaint seeking to stop two related operations and their principals who facilitated billions of illegal robocalls to consumers nationwide, pitching everything from auto warranties to home security systems and supposed debt-relief services. According to the complaint, James "Jamie" Christiano and the companies he controls operated "TelWeb," a computer-based telephone dialing platform that can be used to blast out a large volume of telephone calls––especially robocalls––in a short time. The FTC alleged that, through TelWeb, Jones's operation bombarded consumers with more than one billion illegal robocalls annually. The FTC charges were settled with a $1.35 million judgment.

iv. *FTC vs. Aaron Michael Jones*. The FTC's complaint charged nine individuals and 10 corporate entities with operating robocalling enterprises allegedly controlled by Mike Jones. According to the FTC's complaint, between at least March 2009 and May 2016, the defendants made or helped to make billions of robocalls, many of which sold extended auto warranties, search engine optimization services, and home security systems, or generated leads for companies selling those goods and services. Many of those calls were to numbers on the FTC's

DNC Registry. A court approved a $2.7 million penalty against Jones.

v. *FTC v. Pointbreak Media, LLC*. In May 2018, the FTC alleged that this Florida-based scheme deceived small business owners by falsely claiming to represent Google, falsely threatening businesses with removal from Google search results, falsely claiming that they could associate keywords with these businesses, and falsely promising first-place or first-page placement in Google search results. The defendants ultimately had to pay over $3.3 million.

f. Examples of State Attorneys General Enforcement Actions Under the TSR

i. *50 State Attorneys General Anti-Robocall Litigation Task Force*. In August 2022, the formation of a nationwide Anti-Robocall Litigation Task Force of 50 attorneys general was announced, whose purpose is to investigate and take legal action against the voice providers responsible for bringing a majority of foreign robocalls into the United States. The task force issued 20 civil investigative demands to 20 gateway providers and other entities that are allegedly responsible for a majority of foreign robocall traffic.

ii. *North Carolina Attorney General Complaint Against Articul8*. In January, 2022, the North Carolina Attorney General Josh sued VoIP provider Articul8 and its owner Paul K. Talbot of Texas for allegedly violating the TSR and facilitating illegal and fraudulent telemarketing calls and robocalls that targeted millions of people in the United States and hundreds of thousands of North Carolinians. The complaint alleges that in a period of just a few months in 2020 and 2021, Articul8 routed more than 65 million calls to phone numbers in North Carolina, with some North Carolinians receiving between 50 and 200 calls on a single day.

iii. *Florida Attorney General Complaint Against SmartBiz*. In December, 2022, the Florida Attorney General filed a complaint against Smartbiz Telecom, LLC, alleging that it was responsible for transmitting millions of foreign-based robocalls into the United States. The complaint alleges that Smartbiz, transmitted obviously fraudulent phone traffic, such as calls purporting to be from 911, and profited from illegal scam messages. The complaint notes that the company received more than 250 traceback requests from ITG. The Florida Attorney General's Office is seeking injunctive relief, consumer restitution and civil penalties pursuant to the Florida Deceptive and Unfair Trade Practices Act, the TCPA, and the TSR.

g. Examples of DOJ *Criminal* Enforcement Actions Under the Wire Fraud Statute.

i. *United States v. Andrew Smith, et. al.* The DOJ secured convictions against two individuals who were sentenced to 25 and 20 years in prison for their roles in a $10 million telemarketing scheme that defrauded primarily elderly victims in the United States from call centers in Costa Rica. Andrew Smith and Christopher Lee Griffin were convicted of one count of conspiracy to commit wire fraud, eight counts of wire fraud, one count of conspiracy to commit money laundering and seven counts of international money laundering. The court also ordered Smith to pay $10,222,838.76 in restitution to be paid jointly and severally with his co-conspirators and forfeit $406,324.96. Griffin was ordered to pay $9,612,590.39 in restitution to be paid jointly and severally with his co-conspirators and forfeit $182,439.

ii. *United States v. HGlobal, Sunny M. Joshi, et. al.* The DOJ secured convictions against twenty-one members of a massive India-based fraud and money laundering conspiracy that defrauded thousands of U.S. residents of hundreds of millions of dollars. Among the many charges were conspiracy to commit wire fraud, and the criminals were eventually sentenced to terms of imprisonment up to 20 years. The original indictment charged a total of 61 individuals and entities for their alleged involvement in the scheme.

h. Examples of DOJ Civil Enforcement Actions Against VoIP Providers Under the Wire Fraud Statute.

i. *United States v. Nicholas Palumbo, TollFreeDeals, et. al.* The DOJ alleged that VoIP provider TollFreeDeals was warned numerous times that it was carrying fraudulent robocalls and yet continued to do so. Numerous foreign-based criminal organizations were alleged to have used the defendants' VoIP carrier services to pass fraudulent government- and business-imposter fraud robocalls to American victims. The complaint specifically charged the defendants with wire fraud, and alleged that the company served as a "gateway carrier," making it the entry point for foreign-initiated calls into the U.S. telecommunications system. In securing a preliminary injunction, the court agreed with DOJ "that 'multiple individual victims in the United States suffered significant fraud losses,' and that '[e]very day that the defendants' actions in this vein continue, the public is at risk of harm in the form of additional high-dollar fraud losses.'"

ii. *United States v. Jon Kahem, Global Voicecom, Inc., et. al.* In a similar complaint against a different VoIP provider, the DOJ eventually secured a consent decree that permanently barred the defendants from, among other things, using the U.S. telephone system to: deliver prerecorded messages through automatic means, carry calls to the United States from foreign locations, and provide calling and toll-free services for calls originating in the United States. In addition, the defendants were permanently barred from serving as employees, agents, or

consultants to any person or entity engaged in these activities.

i. Examples of FCC Civil Enforcement Actions Under the Wire Fraud Statute.

i. *Adrian Abramovich, Marketing Strategy Leaders, Inc. et. al*. In addition to fining Adrian Abramovich $120 million for malicious spoofing that was part of a massive robocalling operation, the FCC also determined that he violated the wire fraud statute. In determining the total fine, the FCC took into account that Abramovich's violation of the wire fraud statute demonstrated the "egregiousness of [his] violations, the consumers he harmed, and the scale and scope of his illegal activities."

j. Examples of Federal Enforcement Actions Relating to Fraudulent Lead Generation.

i. *Aaron Michael Jones, et al*. The FCC unanimously adopted a Notice of Apparent Liability (NAL) for Forfeiture of nearly $300 million targeting the so-called Cox/Jones Enterprise that was responsible for more than 5 billion auto warranty robocalls. The FCC alleges that the Cox/Jones Enterprise improperly relied on invalid consent capture pages from vehicle service contract sellers for the calls, and that its clients consistently provided the Enterprise and the ITG with websites that provided little or no disclosure language as proof of consent to make the calls. The FCC further alleges that the Cox/Jones Enterprise never obtained prior express written consent before dialing telemarketing calls to wireless phones, and did not obtain prior express consent before dialing telemarketing calls to residential phones.

ii. *ITMedia Solutions LLC, et. al*. In January 2022, the FTC filed a complaint against ITMedia Solutions LLC, a number of affiliate companies, and their owners and officers alleging that they operated hundreds of websites that were designed to entice consumers into sharing their most sensitive financial information, and then sold that information to marketing companies and others without regard for how the information would be used. The FTC alleged that 84 percent of the loan applications collected through these websites since January 2016 were not sold to lenders, but instead disseminated to an array of marketers, debt relief and credit repair sellers, and companies that would resell consumers' information without regard for how the information would be used. In many instances, ITMedia was not even aware of the purpose for which a company was buying consumers' data, or at times even the physical location of the company.

iii. *Day Pacer LLC, Edutrek LLC, et. al*. In April 2019, the FTC filed a complaint against Day Pacer LLC, Edutrek LLC, and other individual defendants, alleging that they obtained consumers' phone numbers from websites that claimed to help consumers apply for jobs, health insurance, unemployment benefits, Medicaid coverage, or other forms of assistance, and instead of offering these services, the defendants called consumers to market vocational or post-secondary education programs, according to the FTC. Similarly, the complaint alleges that the defendants have purchased leads from

"FindFamilyResources.com," a website offering to provide information about Temporary Assistance to Needy Families (TANF), welfare benefits, and unemployment insurance.