



# USTELECOM'S INDUSTRY TRACEBACK GROUP

Policies and Procedures

January 2020



USTELECOM | THE BROADBAND ASSOCIATION

# Table of Contents

<b>Industry Traceback Group Overview</b> .....	<b>2</b>
Definitions.....	2
ITG Membership Categories.....	5
Traceback Process and Best Practices .....	6
Privacy of Call Traceback Information .....	10
<b>Robocall Sourcing Policy</b> .....	<b>11</b>
Sources to be Utilized for Identifying Calls or Calling Campaigns for Traceback .....	11
<b>Enforcement Agency ListServ</b> .....	<b>12</b>
<b>ITG Record Retention Policy</b> .....	<b>13</b>
<b>Do Not Originate Policy</b> .....	<b>13</b>
DNO Policies from Government Entities.....	14
DNO Policies for Private Enterprises .....	14
Maintaining the Integrity of DNO Implementation .....	15
Effectiveness Linked to Scale of Implementation .....	15
<b>APPENDIX A – Enforcement Agency Handoff</b> .....	<b>16</b>
<b>APPENDIX B – 47 USC 222</b> .....	<b>17</b>
<b>APPENDIX C – Sample Email Templates Sent via Portal</b> .....	<b>18</b>
<b>APPENDIX D – Sample ITG Escalation Letters</b> .....	<b>23</b>

## Industry Traceback Group Overview

These Industry Traceback Group (ITG) Policies and Procedures provide information on the criteria for membership in the ITG and the policies and procedures governing ITG activities. Adherence to the Policies and Procedures will help foster cooperation by a broad range of supportive industry participants (including incumbent local exchange carriers, competitive local exchange carriers, wireless carriers, VoIP providers, long distance companies, and wholesale providers) to enhance the robust protection of voice networks and users of voice services from fraudulent, abusive, and/or unlawful robocalls and to reduce the number of illegal robocalls by helping to identify the source of such calls.

The origination, delivery and termination of robocalls involves numerous voice service providers in a complex ecosystem. Over 100 entities have participated in ITG Traceback of suspected illegal robocalls to date. As described and defined below, voice service providers fall into three broad categories: Cooperative Voice Service Providers (those who are fully cooperative with Tracebacks and meet numerous requirements described herein), Non-Cooperative Voice Service Providers and Call Path Voice Service Providers (those providers in the call path who don't meet the many requirements necessary to be labeled Cooperative Voice Service Provider but who participate in Tracebacks and have not been labeled Non-Cooperative Voice Service Provider).

### Definitions

The following definitions are used throughout the ITG Policies and Procedures:

- **Cooperative Voice Service Provider.** A voice service provider committed to protecting networks and consumers from fraudulent and abusive robocall traffic. A Cooperative Voice Service Provider must agree to, and abide by, all the policies and procedures set forth in this document.
- **Non-Cooperative Voice Service Provider.** A voice service provider that does not follow the best practices contained herein (pages 8-11) and does not cooperate with Cooperative Voice Service Provider(s) or USTelecom on Tracebacks of Suspicious Traffic. Specific actions that will result in designation as “non-cooperative” include the following:

#### *Non-Responsive*

- When a voice service provider that fails to respond within [BEGIN REDACTED] [END REDACTED] business days to [BEGIN REDACTED] [END REDACTED] separate consecutive traceback requests from the ITG despite reasonable efforts to ensure appropriate contact information for the provider and reasonable attempts to reach the provider via email and phone.

### *Ongoing Illegal Origination*

- An Originator is the last (farthest upstream) voice service provider in a Traceback sequence. The Originator may have placed the call itself, or received the call from its customer.
- A. Single Campaign
  - When a voice service provider that, [BEGIN REDACTED] [END REDACTED] or more days after identification by the ITG as an Originator for a particular Campaign, originates calls for that same Campaign.
- B. Multiple Campaigns
  - When a voice service provider that has been identified by the ITG as an Originator for multiple high-volume Campaigns.

### *United States (U.S.) Point of Entry*

- The U.S. Point of Entry is the first downstream voice service provider routing traffic that was originated outside the United States on to the United States Public Switched Telephone Network.
- A. Single Campaign
  - When a voice service provider that, [BEGIN REDACTED] [END REDACTED] or more days after identification by the ITG as the U.S. Point of Entry for a particular Campaign, passes calls for that same Campaign.
- B. Multiple Campaigns
  - When a voice service provider that has been identified by the ITG as the U.S. Point of Entry for multiple high-volume Campaigns.

### *Not Found*

- When a voice service provider whose responses to Traceback requests are entered as “Not Found” for more than [BEGIN REDACTED] [END REDACTED] percent of all responses, absent reasonable explanation.

Note: merely responding to Tracebacks, without taking reasonable steps to eliminate the origination of illegal calls after notification of such calls, is not sufficient to avoid being labeled a Non-Responsive Voice Service Provider.

USTelecom reserves the right to publish the identity of and share information about Non-Cooperative Voice Service Providers. This sharing can be with government enforcement agencies, with other voice service providers, and with the public.

A voice service provider’s classification as “non-cooperative” will be removed if the voice service provider is no longer engaged in any of the above activities in a [BEGIN REDACTED]

[END REDACTED] day period after the ITG has deemed the provider as non-cooperative. Resumption of non-cooperative behavior will result in reclassification as non-cooperative.

- **Call Path Voice Service Provider.** A voice service provider in a call stream path that is neither a Cooperative Voice Service Provider nor a Non-Cooperative Voice Service Provider.
- **Affiliates.** With respect to a specified voice service provider, any other entity that, directly or indirectly through one or more intermediaries, controls, is controlled by or is under common control with the voice service provider specified. For purposes of these principles, the term “control” (including its correlative meanings, “controlled by” and “under common control with”) shall mean possession, directly or indirectly, of the power to direct or cause the direction of management or policies (whether through ownership of securities or partnership or other ownership interests, by contract or otherwise).
- **Campaign.** A group of calls with identical or nearly identical messaging believed to be coming from the same source(s) as determined by the content and calling patterns of the caller. A single Campaign often represents hundreds of thousands or millions of calls.
- **Suspicious Traffic.** Suspicious Traffic is identifiable by a pattern of voice calls that: (1) transit one or more Cooperative Voice Service Provider networks and that (2) have characteristics associated with abusive, unlawful, or fraudulent practices (including, but not limited to, lack of header information, volumetric anomalies, calling or called party information modification, complaints received from called parties, law enforcement, 3<sup>rd</sup> party aggregators, or call transcripts). Cooperative Voice Service Providers shall work collaboratively to further develop this definition on an as-needed basis.
- **Incident Data.** Data sent between Cooperative Voice Service Providers and/or USTelecom relating to Suspicious Traffic that includes the following (where applicable), information: (1) originating telephone number; (2) originating IP address; (3) called telephone number; (4) called IP address; (5) Session Initiation Protocol (SIP) header anomalies; (6) evidence of Caller ID, Automatic Number Identification (ANI), telephone number spoofing; (7) volume of calls, including call detail record (CDR) file(s) information (as applicable); and (8) date and time of calls.
- **Traceback.** A network-based process that begins with the terminating Cooperative Voice Service Provider (or a set of terminating providers) possessing evidence of illegal call activity, seeking out the source of the originating Suspicious Traffic that is coming from a third party network, non-native to their own terminating network. The call is then systematically traced through the non-native networks that chronologically

precede the terminating network(s) until a Non-Cooperative Voice Service Provider and/or the Originator and/or originating customer is identified.

- **Trace Forward.** Trace Forward is intended to address a scam that solicits a victim to call back to complete an attempted scam or fraud. In the Trace Forward process the networks used to initiate the malicious/fraudulent call to the end user are not traced, but rather the network serving the call back telephone number is identified. To trace forward, the ITG administrator contacts the voice service provider that owns the Direct Inward Dial (DID) number and requests information about the customer the number is associated with (name, e-mail, contact information, payment information). The Trace Forward process is repeated until the voice service provider conducting the Trace Forward finds the source/destination.
- **Secure Traceback Portal (STP).** An online portal managed by USTelecom to facilitate Tracebacks and identification of illegal robocall Originators. Call Path Voice Service Providers, Cooperative Voice Service Providers, and Non-Cooperative Voice Service Providers that fall within the call path receive a Traceback request via email. The message includes the call details from the downstream Call Path Voice Service Provider or Cooperative Voice Service Provider and a secure link that logs the user into the portal where they add specific details on the upstream Call Path Voice Service Provider. The link included in the traceback request leads directly to a form where the identity of the next upstream voice service provider is entered.

## ITG Membership Categories

The ITG is comprised of two membership groups consisting of ITG Steering Committee Members and ITG Affiliate Members as described below.<sup>1</sup> In addition to these two broad membership categories, an Executive Committee is responsible for determining the overall direction and activities of the ITG as described below.

### ITG Steering Committee Members

ITG Steering Committee Members implement the Policies and Procedures governing the operational aspects of the ITG and industry Tracebacks. ITG 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 STP and participation in regularly scheduled ITG Member calls; (2) fully comply with the ITG Policies and Procedures contained herein; (3) sign a statement of intent to adopt and follow the Best Practices listed on pages 8-11; and (4) agree to adhere to the principles contained in the State Attorneys General Anti-Robocall Principles available at <https://www.ustelecom.org/wp->

---

<sup>1</sup> A list of ITG members is available at <https://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg>.

<content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf>;<sup>2</sup>

and (5) ensure that the ITG Member and all of its Affiliates adhere to the State AG Anti-Robocall Principles. Any members of the ITG that joined prior to 2019 and who have acted in good faith to implement Tracebacks are eligible to be ITG Steering Committee Members. Subsequent designation is contingent upon a demonstrated adherence to the ITG Policies and Procedures for a prior period of one year. Designation as an ITG Steering Committee Member is subject to the sole discretion of USTelecom, and the one year period may be waived upon approval of the Executive Committee. Membership in the ITG Steering Committee is contingent upon continuous compliance with the requirements above. USTelecom may terminate ITG Steering Committee membership in at any time, and for any reason, in conjunction with the advice of the Executive Committee.

### **ITG Affiliate Members**

ITG Affiliate Members are members of the ITG who participate in industry Tracebacks but are not ITG Steering Committee Members. Any voice service provider may participate in call Tracebacks, and all voice service providers are encouraged to do so, but to be considered an ITG Affiliate Member, an entity must be a Cooperative Voice Service Provider and: (1) participate in quarterly scheduled ITG Member calls; (2) fully comply with the ITG Policies and Procedures; and (3) sign a statement of intent to adopt and follow the best practices listed in the sections below. Categorization as an ITG Affiliate Member is subject to approval by USTelecom in conjunction with the advice of the Executive Committee. Membership in the ITG is contingent upon compliance with the requirements above. USTelecom may terminate ITG Affiliate Membership in the ITG at any time, and for any reason, in conjunction with the advice of the Executive Committee.

### **ITG Executive Committee Members**

The ITG Executive Committee consists of Steering Committee members that support the ITG as Platinum, Gold or Silver-level supporters or USTelecom members that support the ITG as Platinum, Gold, Silver or Bronze-level supporters.<sup>3</sup> The Executive Committee sets the overall direction of the ITG and provides guidance on major ITG decisions.

## **Traceback Process and Best Practices**

**Traceback Initiation and Tracking.** USTelecom initiates the Traceback process in order to identify the origin of an individual call or a Campaign using a source consistent with its Sourcing Policy as described on pages 10-11. A Traceback is initiated by the USTelecom Traceback team

---

<sup>2</sup> Note: For those providers who offer wholesale voice services but do not offer retail service to end-use customers, it is understood that some principles may not apply, including Principle # 1 (Offer Free Call Blocking and Labeling) and Principle #5 (Confirm the Identity of Commercial Customers). To the extent any Principle is inapplicable to an ITG member's business, such information can be provided in the statement of intent required for ITG membership that otherwise acknowledges and endorses the State Attorneys General Principles.

<sup>3</sup> ITG support levels are determined on an annual basis. Participation in the Executive Committee reflects a commitment to the ITG in the form of financial contributions to cover ITG costs.

who enters the minimum information required for a Traceback into the STP. Once the information has been entered, a notification is sent to the terminating voice service provider(s) whose customer(s) received the Suspicious Traffic. That voice service provider then investigates the identity of the upstream voice service provider from whom it received the Suspicious Traffic and enters the information into the STP. If the upstream voice service provider has previously participated in a Traceback, its contact information will be in the STP and can be selected from a drop-down menu. If the upstream provider has not previously participated in a Traceback, contact information for that provider will not be available in the STP. In that case, the downstream voice service provider should provide contact information for the upstream provider, so that the STP can be appropriately updated. If contact information is not available, the USTelecom Traceback team seeks out information to avoid a dead end in the Traceback. This process is repeated for each voice service provider in the call path until the Originator is identified or a dead end is reached. All communications from upstream and downstream voice service providers concerning a Traceback are automatically logged in the STP.

**ITG Communications with Voice Service Providers.** As a call is systematically traced through networks, semi-automated email messages are sent via the STP to voice service providers in the call path. Such messages are standardized but may differ based on the identity and status of the receiving voice service provider, ie., whether a voice service provider is an ITG Member familiar with the process, a new provider who has not previously participated in a Traceback, or a provider that has been unresponsive to prior requests. For examples of each message see Appendix C.

A service provider who has been identified as meeting the criteria associated with being “non-cooperative” under any of the criteria contained in the definition of a Non-Cooperative Voice Service Provider will be sent an email notification via the STP. Different messages are sent depending on whether the provider is non-responsive or has been identified as an Originator or as a provider that is the U.S. Point of Entry for Suspicious Traffic. See Appendix D for escalation letters that are sent to such providers.

#### **“Problem Zone” Message**

A voice service provider identified as an Originator and/or as the U.S. Point of Entry for Suspicious Traffic, will be notified by USTelecom’s Traceback team that they are in danger of being labeled a Non-Cooperative Voice Service Provider unless action is taken to halt the flow of the Suspicious Traffic. Such providers shall be notified of their status and provided with access to reference materials with information on potential mitigation steps that can be taken to stop illegal calling activity and avoid a non-cooperative designation going forward. The STP may be configured in a manner that provides an identifier for such providers, thus putting other voice service providers on alert that an individual voice service provider has been notified that it is in danger of being labeled a Non-Cooperative Voice Service Provider if mitigation steps are not taken.



## **Non-Cooperative Service Provider Message**

If sufficient mitigation steps are not taken and a provider meets the definition of a Non-Cooperative Voice Service Provider, USTelecom's Traceback team will notify the provider through an automated alert of their status and ask that they take the necessary steps to stop the illegal calling activity. Subsequently, the Traceback Team will initiate additional Traceback requests to monitor whether or not Suspicious Traffic has ceased. When an upstream provider has been notified that they have been labeled as non-cooperative, their downstream providers should be notified within 48 hours of their status. The STP may be configured in a manner that provides an identifier for such providers, thus putting other voice service providers on alert that an individual voice service provider has been notified that it is a Non-Cooperative Voice Service Provider.

## **Best Practices**

- 1. Dedicated Point of Contact.** Each Cooperative Voice Service Provider will designate an individual or internal organization as a dedicated point of contact for addressing requests from other Cooperative Voice Service Providers or USTelecom related to Suspicious Traffic as well as a back-up person or internal organization. Each Cooperative Voice Service Provider will provide other Cooperative Voice Service Providers and USTelecom with the full name, title, phone number and e-mail address, and normal business hours of operation for each of their respective points of contact. USTelecom will, upon reasonable request, provide such contact information to enforcement authorities.
- 2. Ongoing Coordination.** Cooperative Voice Service Providers and/or USTelecom will engage in collective coordination regarding instances of Suspicious Traffic, including through the STP. Such coordination between Cooperative Voice Service Providers and/or USTelecom may include electronically exchanging information related to Suspicious Traffic (*e.g.*, through the STP and e-mails), conference calls, or individual outreach between Cooperative Voice Service Providers.
- 3. Prompt Response.** Cooperative Voice Service Providers and/or USTelecom may initiate Traceback investigations into Suspicious Traffic based on reports from a wide range of sources, including end users and other voice service providers, provided that they have a *bona fide* basis to believe that the traffic is Suspicious Traffic. Each Cooperative Voice Service Provider should acknowledge that the Traceback request has been received and is being worked within one business day if received from another Cooperative Voice Service Provider and/or USTelecom relating to Suspicious Traffic, and endeavor to initiate investigation of the source of Suspicious Traffic request within four (4) business hours of acknowledgement as resources permit. The Cooperative Voice Service Provider should strive to complete the investigation and return results within 72 hours from initiation. The reasonableness of a Cooperative Voice Service Provider's response will depend on the context, including whether the Cooperative Voice Service Provider or USTelecom initiating the request identifies such request as urgent to protect consumers from fraud, the complexity of the traffic analysis associated with the request, and the number of outstanding requests received by the Cooperative Voice Service Provider. The

Cooperative Voice Service Provider and/or USTelecom initiating the request has responsibility for following up on the request and ensuring that it is closed out. If a Cooperative Voice Service Provider notifies another Cooperative Voice Service Provider that it sent Suspicious Traffic, it should provide the notified Cooperative Voice Service Provider with the appropriate Incident Data. At a minimum a Cooperative Voice Service Provider investigating Suspicious Traffic originating on, or transiting through its network, should provide USTelecom and all Cooperative Voice Service Provider(s) impacted by and/or involved in the investigation of a specific case (e.g., upstream and downstream parties) with: (1) updates on the status of any investigation into Suspicious Traffic; (2) as-required updates on substantive developments into any investigation into Suspicious Traffic; and (3) resolution of the Suspicious Traffic investigation as outlined in Sections 3(a) and 3(b) below. USTelecom will distribute such information via the STP.

3(a). **Mitigate Traffic Source.** If, after investigation, the notified Cooperative Voice Service Provider learns its own systems and/or end users are generating the Suspicious Traffic, it will (consistent with the terms of its contract with that customer and other relevant legal considerations) take steps to investigate and mitigate calls that are found to be unlawful. If a Traceback investigation results in a finding that that the traffic was lawfully originated, the voice service provider originating the lawful traffic may provide information to Cooperative Voice Service Providers and USTelecom to avoid future investigations into the same customer's traffic. A Cooperative Voice Service Provider that originates traffic from legitimate customers that use autodialers, or that itself initiates autodialed traffic, has the option of informing the rest of the Cooperative Voice Service Providers of the associated traffic patterns so that the others can avoid initiating investigations into that traffic.

3(b). **Investigate Upstream Source.** If, after investigation, the Cooperative Voice Service Provider learns it received the Suspicious Traffic from another Cooperative Voice Service Provider, it should request that the upstream Cooperative Voice Service Provider investigate the Suspicious Traffic. The upstream Cooperative Voice Service Provider should respond promptly to that Traceback request as outlined above in Section 3(a).

4. **Referral to Enforcement Authorities.** In instances where a voice service provider is determined to be a Non-Cooperative Voice Service Provider, relevant information may be forwarded to appropriate federal and state enforcement authorities, including, but not limited to, the Federal Communications Commission, the Federal Trade Commission, the Department of Justice, and state Attorneys General. Cooperative Voice Service Providers may provide such information to enforcement agencies directly or through coordination with USTelecom. Such information should include: (1) the name of the Call Path Voice Service Provider or Non-Cooperative Voice Service Provider; and (2) the circumstances surrounding outreach by the Cooperative Voice Service Provider(s) and/or USTelecom (e.g., date of contact(s); nature of communication from Call Path Voice Service Provider or Non-Cooperative Voice Service Provider). For specific instructions see Appendix A for Enforcement Agency handoff.

4(a). **Special Circumstances.** In instances where a private enterprise and/or enforcement agency sends a Cooperative Voice Service Provider and/or USTelecom a subpoena requesting full call records and data related to their Traceback investigation, a Cooperative Voice Service Provider and/or USTelecom will comply with the subpoena.

5. **Identification of Voice Service Providers.** In addition to law enforcement referrals, USTelecom may also choose to publicly summarize the results of Traceback results for ongoing illegal robocall Campaigns, including the identification of Cooperative Voice Service Providers, Non-Cooperative Voice Service Providers (with sufficient information describing why they have been labeled as such), and Call Path Voice Service Providers. Such identification may be provided to ITG Members and may also include the publication of a dynamic list on a publicly available website, a periodic electronic or written publication, or some other form of tangible publication. Any provider who has been identified as a Non-Cooperative Voice Service Provider will be immediately removed from any such list if information is provided demonstrating they do not or no longer meet the requirements to be labeled “non-cooperative.”

6. **Transmission of Voice Traffic.** Cooperative Voice Service Providers abiding by these best practices may choose to accept voice traffic only from other Cooperative Voice Service Providers and Call Path Voice Service Providers. To ensure that consumers, businesses and voice service providers are protected from illegal and potentially fraudulent actions, and consistent with contractual limitations and legal considerations, Cooperative Voice Service Providers should consider taking appropriate steps to eliminate acceptance of Suspicious Traffic from Non-Cooperative Voice Service Providers.

While ITG members are expected to adhere to the best practices above at ALL times, call traffic, networks, systems, processes, training, and capabilities vary among service providers, as do the potentially illegal calling situations. Therefore, USTelecom acknowledges that these best practices may not apply for every individual Traceback. Any provider who is unable to respond to an individual Traceback should provide sufficient information in the STP as to why it is unable to respond.

**Privacy of Call Trace-Back Information.** No Cooperative Voice Service Provider will share information about a Campaign under investigation provided by another party with any external entity except (i) USTelecom via the STP, (ii) those Call Path Voice Service Providers contacted as part of the Traceback investigation, or (iii) pursuant to a valid legal process, provided however that any individual Cooperative Voice Service Provider that receives any subpoena or other legal mandate seeking information received from another voice service provider shall, to the extent not prohibited by law, promptly inform the voice service provider from which it received information and provide that voice service provider an opportunity to resist providing the requested information. Information gathered by Cooperative Voice Service Providers during such investigations, including customer proprietary network information (CPNI), shall be used solely for the purpose of conducting Suspicious Traffic investigations. Nothing in this privacy section prohibits a Cooperative Voice Service Provider from proactively telling an enforcement agency, consistent with the law and with its own privacy policy, that it has information about a

Campaign that may be of interest to the agency, provided that that Cooperative Voice Service Provider has information about the Campaign learned through its own operations and that it does not disclose information received from other voice service providers or USTelecom absent permission.

In the context of Traceback investigations, USTelecom will share with each downstream Cooperative Voice Service Provider where the investigation ended, including the identity of any Non-Cooperative Voice Service Provider. Nothing in this section shall limit the ability of USTelecom to publicly summarize the results of Traceback results for ongoing illegal robocall Campaigns as described in Section 5 above.

### **Robocall Traceback Sourcing Policy**

The following section outlines the process utilized by USTelecom on behalf of the ITG to identify calls and/or calling Campaigns that are selected for initiation of Tracebacks (“Traceback Candidate”). The principal goal of this effort is to ensure that any Tracebacks initiated by USTelecom are initiated in good faith for the purpose of identifying the source of illegal and/or fraudulent traffic, thereby satisfying the requirements of 47 USC 222(d)(2) (See Appendix B). Specifically, USTelecom’s good faith efforts will ensure that any Traceback undertaken by the ITG is initiated to “protect the rights or property of the voice service provider, or to protect users of those services and other voice service providers from fraudulent, abusive, or unlawful use of, or subscription to, such services.”

#### **Sources to be Utilized for Identifying Calls or Calling Campaigns for Traceback.**

To best ensure that only actionable Traceback Candidates are pursued by the ITG for Traceback, USTelecom is guided by established principles that introduce reasonable due diligence, integrity and transparency into the Traceback process. The principles established by USTelecom dictate that Traceback Candidates will only be shared with the ITG if:

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

Prior to initiating a Traceback, USTelecom will conduct due diligence to warrant utilization of the Traceback process. Traceback Candidates shall be validated by USTelecom and the ITG generally through the following resources, although USTelecom may also independently initiate Tracebacks that satisfy the above referenced criteria.

- **ITG Steering Committee Member Referrals.** Designated ITG Steering Committee Members may identify Traceback Candidates. Any ITG Steering Committee Member identifying such Traceback Candidates shall use good faith efforts to ensure that the

Traceback Candidate satisfies the requirements of 47 USC 222(d)(2) (*e.g.*, calls to an ITG Steering Committee Member's subscribers have been identified as suspected fraud).

- **Analytics Providers.** Many analytic providers (*e.g.*, Nomorobo, YouMail) utilize scoring algorithms to identify suspected fraudulent traffic to their subscribers. USTelecom, on behalf of the ITG, may partner with such analytics providers to help identify Traceback Candidates.
- **Enforcement Authorities.** USTelecom seeks to cooperate with enforcement authorities at the local, state and federal level with the goal of providing such agencies with actionable leads on active Suspicious Traffic campaigns. This cooperation may also include Traceback Candidates identified by appropriate enforcement authorities for whom USTelecom may initiate a Traceback.
- **Enterprises Subject to Scams.** Businesses whose brands are being illegally used in Campaigns without authorization by the business (including, but not limited to, healthcare providers, financial institutions, utilities, technology companies) may request that USTelecom initiate a Traceback on their behalf, subject to conditions and limitations on the use of the Traceback results as established by the ITG. USTelecom may require a fee for such Tracebacks.

### **Enforcement Agency Listserv**

USTelecom will maintain and operate an information sharing resource for federal and state government agencies responsible for enforcement of laws and regulations to prevent illegal Campaigns. Participating agencies will receive information pertaining to illegal Campaigns initiated by the ITG. The ListServ provides information on active Campaigns under investigation by the ITG and serves as a resource to ensure coordination among government agencies.

**Eligibility.** Federal and state government agencies that actively investigate illegal and fraudulent robocalls and who are responsible for enforcement of laws and regulations to prevent illegal robocalls may access the Listserv.

USTelecom will coordinate the ListServ, including adding and removing contacts as necessary. It is the responsibility of federal and state government agencies and law enforcement officials to make sure contact information is up to date.

Eligible agencies include, but are not limited to:

- Federal Communications Commission (FCC)
- Federal Trade Commission (FTC)
- Social Security Administration (SSA)
- State Attorneys General
- Treasury Inspector General for Tax Administration (TIGTA)

Participating on the Listserv will require the use of an official government email address.

The Listserv will only be available to appropriate government officials and USTelecom, who will coordinate with ITG members as necessary.

**Listserv Process.** USTelecom will send notifications of summary reports in real time as Tracebacks are completed or come to a dead-end.

**Process:**

1. Notifications will be sent out with a summary report capturing:
  - a. Description of Campaign
  - b. Campaign ID
  - c. Audio (where available)
  - d. Transcript (where available)
  - e. Call Origin Location
  - f. Start Date of Campaign
  - g. Initial Traceback Report Date
  - h. Volume of calls
  
2. In order to receive the full summary report with all details, a subpoena, CID, or other formal request for details is required. A full report will include:
  - a. Full Call Detail Records as available
  - b. Originator with full details (location, contact information, etc.)
  - c. Additional information related to campaign or the identified Non-Cooperative Voice Service Provider determined to be relevant by USTelecom.

### **ITG Record Retention Policy**

The ITG Record Retention Policy (“the Policy”) is designed to ensure that CDRs associated with any ITG Traceback investigation are retained to assist federal and state enforcement agencies with subsequent investigations and civil or criminal enforcement actions. Individual ITG Steering Committee Members and ITG Affiliate Members have their own internal policies that establish the timeframes for retaining CDRs.

The Policy only applies to CDRs associated with Traceback investigations initiated through the USTelecom STP (“Traceback CDRs”). Under the ITG Record Retention Policy, ITG Steering Committee Members and ITG Affiliate Members’ Traceback CDRs shall be retained by the STP administrator for a period of no less than two years in the STP. For purposes of the ITG Record Retention Policy, the term “retain” shall mean the possession or storage by any method and in any medium, of any record at any location.

## Do Not Originate Policy

This section of the ITG Group Policies and Procedures outlines the policies and procedures to be utilized by USTelecom on behalf of the ITG to implement Do Not Originate (DNO) requests. DNO is a process whereby certain telephone numbers are identified at VoIP gateways or interconnection points, and prevented from terminating to the end user based upon the originating telephone number. A measured and tightly controlled DNO process can be instituted by some or many voice service providers on a voluntary basis. An entity for which a DNO has been instituted (whether a governmental or private entity) shall be referred to hereafter as a DNO Recipient.

### DNO Policies for Governmental Entities

Historically, USTelecom has instituted DNOs on behalf of government agencies at the federal and state level. To qualify to be considered for DNO treatment, a number must: (1) be inbound-only; (2) be currently spoofed by a robocaller to perpetrate impersonation-focused fraud; (3) be the source of a substantial volume of calls (*e.g.* [BEGIN REDACTED] [END REDACTED] or more during a one month period); (4) be authorized for participation in the DNO effort by the party to which the telephone number is assigned; and (5) be recognized by consumers as belonging to a legitimate entity, lending credence to the impersonators and influencing successful execution of the scam. ITG Steering Committee Members, at the direction of USTelecom, shall undertake a volume count of spoofed calls for the previous [BEGIN REDACTED] [END REDACTED] day period. In instances where the volume of spoofed calls exceeds [BEGIN REDACTED] [END REDACTED] during that period, USTelecom may request initiation of the DNO. In consultation with ITG Steering Committee Members, USTelecom may initiate a DNO for a number not meeting the thresholds established for governmental entities if unique and exigent circumstance warrant such action.

- **DNO Implementation is Voluntary.** In an instance where a government agency gains authorization for a DNO, implementation of the DNO by ITG Members is encouraged, but remains voluntary. In an instance where an ITG member chooses to implement a DNO requested by USTelecom, they shall affirmatively report to USTelecom staff that the DNO has been implemented, and its date of implementation.

### DNO Policies for Private Enterprises

In addition to the DNO Policies for governmental entities listed above, the following additional principles shall be applied to private enterprises seeking a DNO from the ITG.

- **Trial Basis; Administrative Charge.** Implementation of DNOs for private enterprises shall only be conducted on a trial basis. USTelecom and ITG Steering Committee Members shall not advertise or promote the availability of such DNOs during this trial period. In addition, USTelecom has the discretion to charge an administrative fee to any private enterprise seeking a DNO.

- **Thorough Vetting.** Both USTelecom and ITG Steering Committee Members shall carefully vet the private enterprise seeking a DNO. Where the private enterprise is a customer of an ITG Steering Committee Member, the ITG Steering Committee Member shall ensure that: (1) the entity requesting the DNO is assigned the number being vetted for a DNO and (2) the private enterprise is a legitimate company active in commerce. Where the private enterprise is *not* a customer of an ITG Steering Committee Member, USTelecom shall undertake similar vetting.
- **Active Event – Volume Thresholds.** A DNO shall only be implemented when the private enterprise is experiencing active and significant fraudulent activity caused by the spoofing of its number. In consultation with the ITG Steering Committee Members, USTelecom may initiate a DNO for a number not meeting the thresholds established for governmental entities if unique and exigent circumstance warrant such action.

**Maintaining the Integrity of DNO Implementation.** No less than twice per year, USTelecom will confirm in writing with each DNO Recipient that the conditions associated with their DNO request (*e.g.*, inbound only number, the number remains assigned to the DNO Recipient) remain in place. Absent written confirmation from the DNO Recipient, USTelecom shall instruct the ITG Steering Committee Members to remove the DNO.

USTelecom shall also maintain a registry of all DNOs that have been implemented (whether for private or governmental entities) by the ITG (“USTelecom DNO Registry”). For each DNO that has been implemented, the USTelecom DNO Registry shall include, at a minimum, the following information: (1) the name of the entity requesting the DNO; (2) the number(s) associated with the DNO; (3) the date of the authorization letter from each DNO Recipient; (4) the names of the ITG Steering Committee Members that have implemented the DNO request; and (5) the date on which the ITG Steering Committee Member implemented the DNO.

ITG Steering Committee Members may request from USTelecom a copy of the USTelecom DNO Registry. In addition, USTelecom at its sole discretion, may share copies of the USTelecom DNO Registry with analytics providers (*e.g.*, First Orion, Hiya, TNS, YouMail, Nomorobo) for implementation in their services. Implementation of DNOs by any such analytics providers shall be reflected in the DNO Registry, in accordance with the above guidelines.

**Effectiveness Linked to Scale of Implementation.** Administratively, it is not feasible to implement DNO for a large group of numbers. Currently DNO is limited to Government agencies (IRS, SSA, etc). Private industry DNOs must be considered only in extreme cases. In order to implement DNO on large quantities of TNs, automated systems and established industry processes are needed to properly manage and implement DNO. Absent these, numbers should remain limited to government agencies.



## **APPENDIX A**

### **ENFORCEMENT AGENCY HANDOFF**

A Cooperative Voice Service Provider and/or USTelecom can assist enforcement authorities and take several actions to prevent fraudulent and abusive robocalls. Outline below is the process for Traceback handoff to specific enforcement agencies that have partnered with the ITG.

- 1. Federal Communications Commission (FCC).** A Cooperative Voice Service Provider and/or USTelecom shall send a written referral on official letterhead containing a brief summary of the Traceback investigation (“Referral Letter”). Such a letter can be in the form of an email communication. The Referral Letter shall not include any CPNI, but may include the names of Non-Cooperative Voice Service Providers. If the FCC sends a Cooperative Voice Service Provider and/or USTelecom a subpoena requesting full CDRs and data specific to the Traceback investigation, the Cooperative Voice Service Provider and/or USTelecom shall comply with such requests.
- 2. Federal Trade Commission (FTC).** A Cooperative Voice Service Provider and/or USTelecom shall send a written referral on official letterhead containing a brief summary of the Traceback investigation (“Referral Letter”). Such a letter can be in the form of an email communication. The Referral Letter shall not include any CPNI, but may include the names of Non-Cooperative Voice Service Providers. If the FTC sends a Cooperative Voice Service Provider and/or USTelecom a Letter of Inquiry requesting full CDRs and data specific to the Traceback investigation, the Cooperative Voice Service Provider and/or USTelecom shall comply with such requests.

**Agencies other than the FCC and FTC.** A Cooperative Voice Service Provider and/or USTelecom may handoff Traceback information to a federal or state enforcement authority. When an enforcement agency requests information pertaining to a specific Traceback investigation, a Cooperative Voice Service Provider and/or USTelecom will send a referral on official letterhead providing a brief summary of the Traceback investigation. (“Referral Letter”). Such a letter can be in the form of an email communication. If the enforcement agency sends a Cooperative Voice Service Provider or USTelecom a subpoena or Letter of Inquiry requesting full CDRs and data specific to the Traceback investigation, the Cooperative Voice Service Provider or USTelecom shall comply with such requests.

To the extent that any federal or state agency has a different or unique process than that described above, this Appendix will be updated accordingly.

Note: The Enforcement Agency ListServ operated by USTelecom as described in these Policies and Procedures serves as a method by which USTelecom will submit referrals.

**APPENDIX B**  
**47 USC 222.**

**47 U.S.C. § 222 -Telecommunications § 222: Privacy of Customer Information**

**(a) In general**

Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

**(b) Confidentiality of carrier information**

A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

**(c) Confidentiality of customer proprietary network information**

**(1) Privacy requirements for telecommunications carriers**

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

**(2) Disclosure on request by customers**

A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

**(3) Aggregate customer information**

A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefor.

**(d) Exceptions**

Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents--

**(1)** to initiate, render, bill, and collect for telecommunications services;

**(2)** to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

**APPENDIX C**  
**SAMPLE EMAIL TEMPLATES SENT VIA PORTAL**

***FORMAL EMAIL TO NEW PROVIDERS WHO HAVE NEVER PARTICIPATED IN A TRACEBACK***

To Whom It May Concern:

By way of introduction, my name is XXX, and I coordinate the efforts of USTelecom's Industry Traceback Group (ITG). We are writing to request your assistance with industry efforts to protect consumers from fraudulent, abusive or potentially unlawful robocalls. My contact information is listed below, and I would be more than happy to discuss this request with you over the phone.

A member of USTelecom's ITG recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin (call details with date(s) are listed below). We request that you assist industry stakeholders who are engaging in traceback efforts in order to help identify the source of this potentially fraudulent, abusive or unlawful network traffic. To assist us in our efforts, **we are asking that you respond to this traceback inquiry as soon as possible, but no later than three business days from now.**

USTelecom, a 501(c)(6) trade association that represents service providers and suppliers for the telecommunications industry, leads the ITG, a collaborative effort of companies from across the wireline, wireless, VoIP and cable industries that actively trace and identify the source of illegal robocalls. The ITG coordinates with carriers at all levels within the call path seeking to identify the source of and eliminate illegal robocall traffic. The ITG also coordinates with federal and state law enforcement agencies to identify non-cooperative providers so they can take enforcement action, as appropriate. For more information about the ITG or a list of the current members, see <https://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg>.

The ITG operates under the auspices of the Communications Act which permits telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information. Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." In addition, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of the ITG, disclosure of information responsive to call tracebacks fits within that exception.

The Federal Communications Commission's (FCC) Enforcement Bureau has sent letters to carriers that have been non-responsive to ITG traceback requests. The letters "urge" carriers to "to cooperate with the USTelecom Industry Traceback Group's program aimed at identifying

the source of illegal robocalls and harmful spoofed calls.” The ITG has received recognition at all levels of government, including the FCC, the Federal Trade Commission (FTC) and all 50 State Attorneys General.

We are asking that you submit your response to this inquiry via our secure on-line portal, where you can see additional detail about all traceback requests involving your network. With respect to the call details below, please provide us with the following:

1. Please investigate the source of this traffic and respond with the identity of the upstream carrier(s) that sent the traffic into your network, or if one of your end users originated the traffic, please identify that end user. **We ask that you use the link below to access the portal and use the drop-down selector to provide this information.**
2. If, in investigating this traffic, the end user(s) originating the traffic are able to demonstrate to you that the traffic complies with applicable United States laws and regulations, please respond via email to me with the description of the traffic, the identity of the customer, and the customer’s explanation.
3. As you investigate this matter, please take appropriate action on your network to ensure compliance with applicable United States laws and regulations, and inform me of the action you have taken.

To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom will provide information to downstream carriers to advise them that suspected illegals on your network continue to be allowed notwithstanding the identification of such calls via the traceback process. Similarly, USTelecom may advise the appropriate law enforcement agencies of such information so that they can take appropriate action, should they elect to do so. Similarly, if this industry effort fails to trace these calls to their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to contact me should you have any questions, or would like to discuss.

Best Regards,

XXX, XXX, USTelecom – The Broadband Association

**Submit your response via our secure on-line portal:**

**<https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=Hddj6k> (URL is a private login; do not share.) Call Details for Incident #123(3d18h ago)**

Date/Time: 2019-00-00 00:00:00 UTC

To: +15555555555

From: +15555555555  
Campaign: XXX

**ITG MEMBER EMAIL**

This is a request for call detail information from the USTelecom Industry Traceback Group regarding a suspected illegal robocall.

Please use the link below to access the Traceback Secure Web Portal and fill in the requested information regarding the source of the call(s).

We would appreciate a response as quickly as possible; ideally in 4 hours or less and no longer than one business day.

This notice was sent to 3 email addresses, including this one.

For help or questions, email [traceback-notice@ustelecom.org](mailto:traceback-notice@ustelecom.org) or call 202-326-7273.

Best Regards,

XXX, XXX, USTelecom – The Broadband Association

**Submit your response via our secure on-line portal:**

**<https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=Hddj6k> (URL is a private login; do not share.) Call Details for Incident #123(3d18h ago)**

Date/Time: 2019-00-00 00:00:00 UTC  
To: +15555555555  
From: +15555555555  
Campaign: XXX  
Summary of campaign

**NON-ITG MEMBER COOPERATING CALL PATH PROVIDER EMAIL TEMPLATE**

Dear Voice Service Provider:

Given your past support of the Industry Traceback Group (ITG), we are writing to inform you that a member of USTelecom's ITG received traffic deemed suspicious from your network (call details with date(s) are listed below). We request that you assist industry stakeholders who are engaging in traceback efforts in order to help identify the source of this potentially fraudulent, abusive or unlawful network traffic. We would appreciate a response to this traceback inquiry in three business days or sooner, but please let us know if you need additional time.

You can respond by clicking the link below, which will take you to our secure traceback portal. There, you can indicate who sourced the call(s) to you.

Feel free to give us a call or reach out to us with any questions, and we appreciate your continued support of ITG efforts.

Best Regards,

XXX, XXX, USTelecom – The Broadband Association 601 New Jersey Avenue NW, Suite 600  
Washington, DC 20001

**Submit your response via our secure on-line portal:**

**<https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=Hddj6k> (URL is a private login; do not share.) Call Details for Incident #123(3d18h ago)**

Date/Time: 2019-00-00 00:00:00 UTC

To: +15555555555

From: +15555555555

Campaign: XXX

Summary of campaign

***NON-RESPONSIVE PROVIDER EMAIL TEMPLATE***

To Whom It May Concern:

We are writing to alert you to problematic telephone calls that have been traced back to your network.

We have notified you multiple times about suspected illegal robocall activity on your network, but we have not received the information we requested with respect to previous call examples. Therefore, we have marked you as a non-responsive voice service provider in our database. This means that we will terminate traceback efforts at your network and mark you as the originator for each traceback to which you have been non-responsive. However, we will continue to send you these notices as new call examples appear to make sure you are aware of the traffic.

We have included a link below so that you can access details about the call(s). Our expectation is that you will determine the source of the traffic and take effective steps to mitigate it. If you

would like to participate in the traceback process, please let us know by responding to this email. We will adjust your designation in our system so that you can provide call source details.

As we have previously indicated, for illegal traffic that goes unmitigated, USTelecom advises downstream providers to whom you send calls and the appropriate law enforcement agencies so they can take appropriate action, should they elect to do so.

Best regards,

XXX, XXX, USTelecom – The Broadband Association 601 New Jersey Avenue NW, Suite 600  
Washington, DC 20001

**Submit your response via our secure on-line portal:**

**<https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=c03YHQG> (URL is a private login; do not share.)**

**Submit your response via our secure on-line portal:**

**<https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=Hddj6k> (URL is a private login; do not share.) Call Details for Incident #123(3d18h ago)**

Date/Time:	2019-00-00 00:00:00 UTC
To:	+15555555555
From:	+15555555555
Campaign:	XXX

## APPENDIX D SAMPLE ESCALATION LETTERS

### ***NON-RESPONSIVE ESCALATION TEMPLATE***

- Message sent when a provider has failed to respond within [BEGIN REDACTED] [END REDACTED] business days to [BEGIN REDACTED] [END REDACTED] consecutive traceback requests.

Date

Dear XXX,

As a result of your non-responsiveness to our repeated written traceback requests, USTelecom – The Broadband Association (USTelecom) is prepared to send a copy of this notice to your downstream providers (as identified in our tracebacks) and appropriate federal and state enforcement authorities to make them aware of your non-cooperation with the Industry Traceback Group (ITG) traceback requests. We also reserve the right to publicly identify your company as non-responsive to industry traceback requests as a resource to other voice service providers and federal and state enforcement agencies. If you believe our traceback requests were in error, or if you have any information to share with us concerning the traceback requests, please respond to this letter within 48 hours of receipt. I can be reached at the address, email or phone number listed below.

As you should be aware from our previous written correspondence, USTelecom<sup>4</sup> manages and operates the ITG, a nationally recognized industry group that was formed to identify the origin of suspected illegal robocalls through cooperative traceback efforts. The ITG includes a broad range of industry participants<sup>5</sup> who work collaboratively to reduce the number of fraudulent and illegal robocalls consumers receive by: 1) identifying the origin of such calls; 2) working with voice service providers to eliminate illegal calls from originating on or traversing their networks where possible; and 3) notifying enforcement authorities of the source of illegal robocalling campaigns.

The Federal Communications Commission (FCC) has encouraged all providers to join this industry initiative and to participate in the traceback efforts of the ITG. The FCC's Enforcement

---

<sup>4</sup> USTelecom, a 501(c)(6) trade association, represents service providers and suppliers for the telecommunications industry (available at [www.ustelecom.org](http://www.ustelecom.org)).

<sup>5</sup> ITG members include ILECs, CLECs, wireless carriers, VoIP providers, long distance companies, and wholesale providers. (available at <https://www.ustelecom.org/the-ustelecom-industry-traceback-group-itg/>).



Bureau has sent letters to carriers that have been non-responsive to ITG traceback requests.<sup>6</sup> The letters “urge” carriers to “to cooperate with the USTelecom Industry Traceback Group's program aimed at identifying the source of illegal robocalls and harmful spoofed calls.” Some of those letters were sent pursuant to the FCC’s authority under Section 403 of the Communications Act, which permits it to institute an enforcement inquiry on its own motion.<sup>7</sup>

The FCC’s exercise of its Section 403 authority in the context of these letters indicates that the agency may be closely investigating the activities of voice providers suspected of generating illegal robocalls, and whether enforcement actions may be necessary.

Every day, the ITG traces back individual call examples from the most prolific illegal calling campaigns. Through that process we have notified you of your company’s handling traffic associated with numerous of these campaigns in an effort to prevent the origination of illegal calls. Our objective analysis<sup>8</sup> has identified your company as originating or transiting a high volume of suspected illegal robocall calls.

In our prior correspondence to you identifying suspected illegal robocall traffic, for each traceback request, we provided you with: 1) the date and exact time of the call; 2) the called number; 3) the calling number (likely spoofed); 4) the downstream carrier to whom you passed your traffic; 5) a description of the illegal campaign associated with the call; 6) a link to our secure, easy to use online portal; 7) the provider serving the called party; 8) whether the called number is on the national do-not-call-list; and 9) in most cases a link to an audio recording capturing what the caller said via an automated or pre-recorded voice. To date, despite your possession of this detailed and ample information,<sup>9</sup> you have never responded to any of these legitimate and reasonable traceback requests. This is both alarming and inconsistent with the

---

<sup>6</sup> See, Letter from Rosemary C. Harold, Chief, Enforcement Bureau, FCC, and Eric Burger, Chief Technology Officer, FCC, to Jonathan Spalter, President & CEO, USTelecom – The Broadband Association (Nov. 6, 2018), *available at* <https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf> (last visited August 13, 2019).

<sup>7</sup> See *e.g.*, Letter from Rosemary C. Harold, Chief, Enforcement Bureau, FCC, and Eric Burger, Chief Technology Officer, FCC, to Ryan Brosnahan, CEO, R Squared (Nov. 6, 2018), *available at* <https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf> (last visited August 13, 2019).

<sup>8</sup> Because the ITG commences its traceback investigations starting at the termination point of any given call, it has no indication as to the specific upstream carriers that will be involved in any given call path. As such, ITG investigations are entirely premised on the facts and conditions associated with each particular traceback and are not influenced by subjective criteria.

<sup>9</sup> The numerous categories of data referenced above, which were provided to you on multiple occasions, include sufficient information for your company to quickly and efficiently trace back the call in question, and to confirm the illegal nature of the call. As we noted in our correspondence to you, Section 222(d)(2) of the Communications Act permits a telecommunications carrier to disclose CPNI in order to “protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.” 47 U.S.C. § 222(d)(2). Despite the ample information we provided, and the legal authority provided to you to share such information, you have declined to do so.

FCC's clear guidance to carriers to support the efforts of the ITG. By our statistical analysis, each of these call examples is indicative of one to two million similar calls.

Our strong desire is to work cooperatively with all voice service providers by providing them with actionable information so they can address suspected illegal calls originating on, or transiting their networks. The ITG's goal is to shut down illegal robocalling campaigns, but this requires a collaborative effort among all industry participants, including your company. We expect your collaboration and assistance on this important issue, but will proceed accordingly should we not hear back from you within the timeframes identified above.

Sincerely,

XXX, XXX, USTelecom – The Broadband Association 601 New Jersey Avenue NW, Suite 600  
Washington, DC 20001

***NON-COOPERATIVE DANGER ZONE MESSAGE (YELLOW IDENTIFIER IN STP)***

- Message sent to voice service provider that has been identified as a call originator and/or U.S Point of Entry but has not yet met the criteria as a Non-Cooperative Voice Service Provider.

To Whom It May Concern:

This is an automatically generated notice alerting you to your change in status as reflected in our Industry Traceback Group on-line portal.

Your status is now YELLOW. A provider in this status has, within the past [BEGIN REDACTED] [END REDACTED] days, been identified as:

- A. An Originator: the last (furthest upstream) voice service provider in a traceback sequence for an illegal robocall. The originator may have placed the call itself, or received the call from its customer, OR
- B. The US Point of Entry: the first downstream voice service provider routing an illegal robocall that was originated outside the US to the US Public Switched Telephone Network (PSTN).

Call details are viewable in our on-line portal at this URL:  
<http://traceback.ustelecom.org/unique-link-details-here>.

You previously received a traceback notice about this traffic; we ask that you immediately follow up with the source to take effective mitigation steps.

Other service providers will be able to view your status in our on-line traceback portal and in email alerts.

There are two conditions that could advance you to the RED status and cause you to be designated as a Non-Cooperative Voice Service Provider:

1. Serving as the Originator or US Point-of-Entry for another illegal call associated with a different calling campaign, OR
2. Serving as the Originator or US Point-of-Entry for the SAME campaign, [BEGIN REDACTED] [END REDACTED] or more days subsequent to notification of the first call for that campaign.

USTelecom reserves the right to publish the identity of and share information about Non-Cooperative Voice Service Providers. This sharing can be with government enforcement agencies, with other voice service providers, and with the public.

Do not hesitate to contact me should you have any questions or would like to discuss. You can respond via reply email or call [BEGIN REDACTED] [END REDACTED].

Best Regards,

XXX, XXX, USTelecom – The Broadband Association 601 New Jersey Avenue NW, Suite 600  
Washington, DC 20001

***NON-COOPERATIVE VOICE SERVICE PROVIDER MESSAGE (RED IDENTIFER IN STP)***

To Whom It May Concern:

This is an automatically generated notice alerting you to your change in status as reflected in our Industry Traceback Group on-line portal.

**You have been designated a Non-Cooperative Voice Service Provider and your status is now RED.** A provider in this status has, within the past [BEGIN REDACTED] [END REDACTED] days, been identified as:

- A. Serving as the Originator or US Point-of-Entry for illegal calls associated with two different calling campaigns, OR
- B. Serving as the Originator or US Point-of-Entry for a given illegal robocall campaign, [BEGIN REDACTED] [END REDACTED] or more days subsequent to notification of the first call for that campaign.

Call details are viewable in our on-line portal at this URL:  
<http://traceback.ustelecom.org/unique-link-details-here>.

You previously received a traceback notice about this traffic; we ask that you immediately follow up with the source to take effective mitigation steps.

Other service providers will be able to view your status in our on-line traceback portal and in email alerts.

USTelecom reserves the right to publish the identity of and share information about Non-Cooperative Voice Service Providers. This sharing can be with government enforcement agencies, with other voice service providers, and with the public. You can provide additional information that you would like to share regarding this matter in the online portal or with USTelecom staff.

Do not hesitate to contact me should you have any questions or would like to discuss. You can respond via reply email or call [BEGIN REDACTED] [END REDACTED].

Best Regards,

XXX, XXX, USTelecom – The Broadband Association 601 New Jersey Avenue NW, Suite 600  
Washington, DC 20001

**CHANGE IN STATUS MESSAGE**

- Message generated to downstream providers identified as exchanging traffic with an upstream provider who has been identified as a Non-Cooperative Voice Service Provider (Red) or a provider that has been identified as exhibiting behavior that may lead to a formal designation as a Non-Cooperative Voice Service Provider (Yellow)

To Whom It May Concern:

This is an automatically generated notice alerting you to a change in status for one of the upstream providers from whom you have recently accepted illegal robocall traffic.

ABC Telecom status has changed to YELLOW.

(or ABC Telecom has been designated a Non-Cooperative Voice Service Provider and now is in RED status)

Details regarding your upstream providers are viewable in our on-line portal at this URL: <http://traceback.ustelecom.org/unique-link-details-here>.

We have sent a separate notice to the provider alerting them to their status change. We ask that you work with the provider to take effective mitigation steps.

Do not hesitate to contact me should you have any questions or would like to discuss. You can respond via reply email or call [BEGIN REDACTED] [END REDACTED].

Best Regards,

XXX, XXX, USTelecom – The Broadband Association, 601 New Jersey Avenue NW, Suite 600, Washington, DC 20001