

**INDUSTRY  
TRACEBACK  
GROUP**

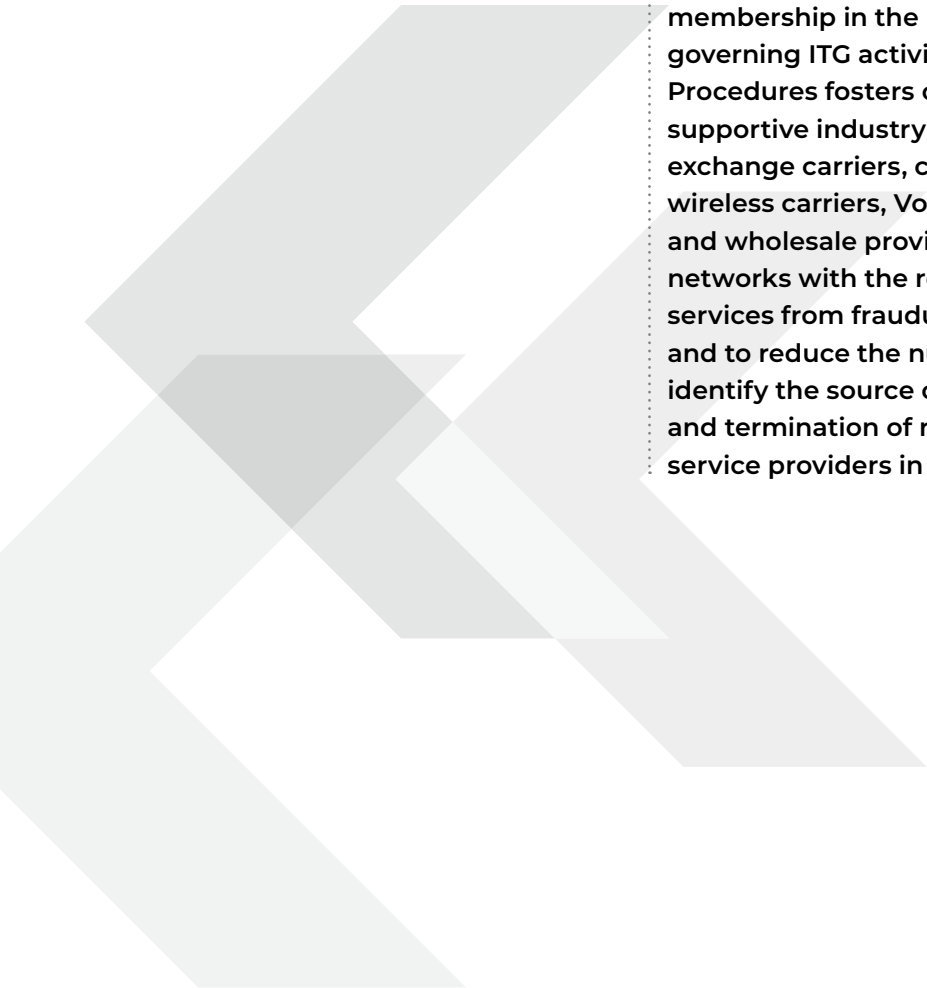
---

# POLICIES AND PROCEDURES

REVISED APRIL 2022

INDUSTRY  
**TRACEBACK** <<<  
GROUP

# 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 fosters 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 trust of voice networks with the robust protection of 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.<sup>1</sup>

# TABLE OF CONTENTS

Article 1: Definitions.....	4
Article 2: ITG Structure and Membership.....	6
Article 3: Traceback Process .....	8
Article 4: Robocall Traceback Sourcing Policy.....	10
Article 5: Working with Enforcement Agencies .....	12
Article 6: ITG Record Retention Policy .....	14
Appendix A: Provider Traceback Best Practices .....	15
Appendix B: Do Not Originate Policy.....	17
Endnotes .....	19



## ARTICLE 1: DEFINITIONS

THE FOLLOWING DEFINITIONS are used throughout the ITG Policies and Procedures:

1. **Voice Service Provider.** A provider of voice service, meaning any service that is interconnected with the public switched telephone network (PSTN) and that furnishes communications to an end user using resources from the North American Numbering Plan. A Voice Service Provider may be located in the United States or be foreign. In general, the ITG will consider to be the same Voice Service Provider any entities that, directly or indirectly through one or more intermediaries, control, are controlled by, or are under common control with the other.<sup>2</sup>
2. **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.
3. **Non-Cooperative Voice Service Provider.** A Voice Service Provider that does not follow the best practices contained in Appendix A and does not cooperate with Cooperative Voice Service Providers or the ITG on Tracebacks of Suspicious Traffic. The ITG will consider a Voice Service Provider non-cooperative based on a variety of factors, including whether the Provider routinely fails to respond to Traceback requests in a timely fashion; is the originating network of illegal robocalls; serves as the U.S. Point of Entry (POE) or Foreign Point of Departure for illegal robocalls; and fails to find records to respond to Traceback requests, among other factors. In addition, 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-Cooperative Voice Service Provider. The factors will be applied uniformly to all Voice Service Providers, and the ITG reserves the sole discretion to determine whether a Provider is non-cooperative based on the factors.
4. **U.S. Point of Entry.** The U.S. POE is the Voice Service Provider identified by the ITG in a Traceback as the first Voice Service Provider within a call's path to take an illegal robocall from a foreign Voice Service Provider (*i.e.*, the Foreign Point of Departure), and place the call on to the U.S. PSTN. In some instances, a call will originate internationally and arrive in the U.S. only to leave the U.S. and return to the U.S. via another Voice Service Provider. In such instances, two U.S. POEs may be identified.
5. **Foreign Point of Departure.** The Voice Service Provider that immediately precedes the U.S. POE. The ITG may consider a Voice Service Provider to be foreign based on several factors that, considered together, indicate that the Voice Service Provider is not in fact owned, controlled, and/or operated by individuals in the United States. Information contained in an FCC Form 499 filing will be considered but is not dispositive.
6. **Campaign.** A group of calls with identical or nearly identical messaging as determined by the content and calling patterns of the caller. A single Campaign often represents hundreds of thousands or millions of calls.

7. **Suspicious Traffic.** Suspicious Traffic is identifiable by a pattern of voice calls that: (1) transit one or more Voice Service Provider networks and (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, third-party aggregators, or call transcripts).
8. **Incident Data.** Data sent between Voice Service Providers and/or the ITG relating to Suspicious Traffic that can include but is not limited to the following information:
  - *originating telephone number;*
  - *originating IP address or Originating and Destination Point Codes;*
  - *called telephone number;*
  - *called IP address;*
  - *Session Initiation Protocol (SIP) header anomalies;*
  - *evidence of Caller ID, Automatic Number Identification (ANI), telephone number spoofing;*
  - *volume of calls, including call detail record (CDR) file information;*
  - *date and time of calls; and*
  - *Information about Voice Service Providers in the call path.*
9. **Traceback.** A network-based process that seeks out the source of Suspicious Traffic. Beginning at a terminating Voice Service Provider, a call is systematically traced from one Voice Service Provider to the preceding Voice Service Provider networks until a Non-Cooperative Voice Service Provider and/or the originating Voice Service Provider or originating customer is identified.
10. **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 (such as name, e-mail, contact information, and payment information). The Trace Forward process is repeated until the Voice Service Provider conducting the Trace Forward finds the source/destination.
11. **Secure Traceback Portal (STP).** An online portal managed by the ITG to facilitate Tracebacks and identification of illegal robocall originators.



## **ARTICLE 2: ITG STRUCTURE AND MEMBERSHIP**

THE ITG IS COMPRISED OF two membership groups consisting of ITG Steering Committee Members and ITG Affiliate Members as described below. 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. The Executive Committee consists of select ITG Steering Committee Members.

In general, only U.S.-based, Cooperative Voice Service Providers will be accepted as members. However, at the sole discretion of the ITG and with the approval of the Executive Committee, exceptions may be made.

### **ITG Steering Committee Members**

ITG Steering Committee Members implement the Policies and Procedures governing the operational aspects of the ITG and industry Tracebacks. Any prospective ITG Steering Committee Member must: (1) be a Cooperative Voice Service Provider that shows a continuous commitment to the Traceback process, including support for Tracebacks 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 in Appendix A; (4) agree to adhere to the principles contained in the State Attorneys General Anti-Robocall Principles;<sup>3</sup> and (5) ensure that it and all of its affiliates adhere to the State Attorneys General Anti-Robocall Principles. Designation as an ITG Steering Committee Member is in the sole discretion of the ITG and is contingent on a demonstrated adherence to the ITG Policies and Procedures for a prior period of six months, which can be shortened or waived upon approval of the Executive Committee. For example, the ITG may waive the six month period for a Voice Service Provider that is U.S.-based, has filed an accurate Form 499 with the FCC, and has not been identified in the STP as the originating Voice Service Provider or U.S. POE for any Tracebacks within the prior six months. The ITG also may consider additional Traceback-related information in its consideration, including the provider's close proximity to originating Voice Service Providers, U.S. POEs, and Non-Cooperative Providers in Tracebacks.

### **ITG Affiliate Members**

ITG Affiliate Members are members of the ITG that participate in industry Tracebacks but are not ITG Steering Committee Members. To qualify as Affiliate Member, a Provider must (1) be a Cooperative Voice Service Provider; (2) participate in quarterly scheduled ITG Member calls; (3) fully comply with the ITG Policies and Procedures; and (4) sign a statement of intent to adopt and follow the best practices listed in Appendix A. Designation as an ITG Affiliate Member is in the sole discretion of the ITG.

Any Voice Service Provider that has previously been identified in the STP as the originating Voice Service Provider or U.S. POE for any Tracebacks within the prior six months will be eligible to join the ITG as an Affiliate Member only after the Provider has

completed a 60 day period in which it is not the originating Voice Service Provider or U.S. POE for any Tracebacks in the STP. The ITG also may consider additional Traceback-related information in its consideration, including the provider's close proximity to originating Voice Service Providers, U.S. POEs, and Non-Cooperative Providers in Tracebacks.

### **ITG Executive Committee Members**

The ITG Executive Committee consists of Steering Committee members that financially support the ITG at specified levels. In conjunction with ITG staff, the Executive Committee sets the overall direction of the ITG and provides guidance on major ITG decisions.

### **Membership Termination and Suspension**

Membership in the ITG is a privilege, not part of any regulatory requirement. ITG members have a responsibility to be models in the fight against illegal robocalls. Accordingly, the ITG, with the advice of the Executive Committee, may terminate the membership of any ITG member for cause. Cause includes, but is not limited to, the member's failure to adhere to these Policies and Procedures or routinely appearing as the originating Voice Service Provider or U.S. POE for Tracebacks. Should the ITG move to remove a member, that member shall have the opportunity to present to the ITG staff and the Executive Committee reasons why it should be allowed to remain a member of the ITG. Termination does not foreclose later reinstatement as a member of the ITG.

In addition, any ITG member that has been alleged to be responsible for illegal robocalls in a government enforcement action, including but not limited to a formal complaint, Notice of Apparent Liability, or cease-and-desist from a federal or state government agency, will be automatically suspended from ITG business. Suspension includes removal of that provider from all references on the ITG's websites and other public materials, ITG member meetings, and ITG member communications and distribution lists. Upon resolution of the enforcement action, such member may request to end the suspension by presenting to the ITG staff and the Executive Committee reasons why it should be reinstated. The ITG, with the advice of the Executive Committee, then will decide whether to reinstate the provider's membership. Membership that is suspended for more than one year will be automatically terminated, though nothing forecloses the provider from seeking membership again in the future after the resolution of the enforcement action.



## **ARTICLE 3: TRACEBACK PROCESS**

### **Traceback Initiation and Tracking**

The ITG initiates the Traceback process to identify the origin of an individual call or a Campaign using a source consistent with its sourcing policy as described below. Once the information required for a Traceback has been entered in the STP by the ITG's traceback team, a notification is sent to the terminating Voice Service Provider whose customer received the Suspicious Traffic. Each Voice Service Provider in the call path then determines the identity of the upstream Voice Service Provider from whom it received the Suspicious Traffic and enters the information into the STP. If an upstream Voice Service Provider is not in the STP, the downstream Voice Service Provider supplies contact information for it so that the STP can be appropriately updated. Providers are expected to have current and correct contact information for those from whom they accept traffic. The process continues until the originating Voice Service Provider 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. If a Voice Service Provider does not respond promptly to a Traceback request, the Traceback is automatically closed. Call path hops will be designated in the STP as follows:

- ▶ No Response, if a Voice Service Provider fails to respond to the Traceback in a timely and complete manner;
- ▶ U.S. Origin, for a U.S.-based Voice Service Provider that originated the call;
- ▶ International Origin, for a foreign-based Voice Service Provider that originated the call;
- ▶ U.S. Point of Entry;
- ▶ Foreign Point of Departure; or
- ▶ Not Found, if a Voice Service Provider is unable to find the requested information.

### **ITG Communications with Voice Service Providers**

As a call is systematically traced through networks, semi-automated email notifications 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 and its cooperation with the ITG.

### **Identification of Voice Service Providers**

In addition to law enforcement referrals, the ITG may also choose to publicly summarize the aggregate results of Tracebacks of illegal robocall Campaigns, including but not limited to the identification of Cooperative Voice Service Providers and Non-Cooperative Voice Service Providers. Such identification may be provided to ITG Members and/or published through the ITG's website, notifications in the STP, email notifications to Voice Service Providers, a periodic electronic or written publication, or some other form of tangible publication. Any Provider that has been identified as a Non-Cooperative



Voice Service Provider will be removed from any such list if information is provided demonstrating that it does not meet, or no longer meets, the Non-Cooperative Voice Service Provider definition.

### **Traceback Confidentiality**

The ITG typically will only share with each downstream Voice Service Provider where the investigation ended, including the identity of any Non-Cooperative Voice Service Provider. Nevertheless, nothing in this section shall limit the ability of the ITG to refer Tracebacks to enforcement authorities and publicly summarize the aggregate results of Tracebacks of illegal robocall Campaigns. The ITG also reserves the right to publish the identity of and share information about Non-Cooperative Voice Service Providers. This sharing can be with but is not limited to government enforcement agencies, other Voice Service Providers, and the public.

### **Organization Traceback Requests**

The ITG may, at times, initiate a Traceback at the request of a non-governmental organization, including an ITG Member. Such Tracebacks may be for the reactive purpose of protecting the organization from illegal or abusive calls that are directly impacting it or its customers or that otherwise damage its reputation. In the case of ITG Members, the purpose of such Tracebacks can include the protection of the Voice Service Provider's rights or property, or to protect users of voice services and other Voice Service Providers from fraudulent, abusive, or unlawful use of, or subscription to, such services. Information regarding a Traceback will be made available to the organization that requested the Traceback investigation in a limited manner and in compliance with applicable law. The ITG will make information available to the organization regarding the caller and originating provider; based on the ITG's discretion, the ITG will only share additional information about the call path where necessary to address the illegal or abusive calls. The recipient of such information may use and share the information only for the purpose of stopping the harmful traffic, including, as appropriate, making referrals to law enforcement agencies. As further described below, except in the case of exigent circumstances, appropriate legal process is required before the ITG discloses specific customer or call records to law enforcement agencies.

All requests to provide information for Traceback investigations requested by an organization will include a certification of customer consent to the disclosure of information or information about why such disclosure is necessary to protect the rights or property of an organization, including a Voice Service Provider, or to protect users of telecommunications services and other Voice Service Providers from fraudulent, abusive, or unlawful use of, or subscription to, such services.<sup>4</sup>

Neither the ITG nor its representatives may disclose information obtained from a Traceback initiated at the request of a private organization to any outside entity without the authorization of the organization that initiated the Traceback investigation, except as necessary to perform the Traceback or as required by law. The Traceback results, however, may be included in aggregated information the ITG provides.



## ARTICLE 4: ROBOCALL TRACEBACK SOURCING POLICY

THIS SECTION OUTLINES THE PROCESS utilized by the ITG to identify calls and/or calling Campaigns that are selected for Tracebacks. The principal goal of this effort is to ensure that any Tracebacks initiated by the ITG are initiated in good faith for the purpose of identifying the source of illegal, fraudulent, or otherwise abusive traffic, thereby satisfying the requirements of 47 USC 222(d)(2). Specifically, the ITG'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" or with the approval of the customer of the voice service.

### Sources Utilized for Identifying Calls or Calling Campaigns for Traceback

To best ensure that only actionable Traceback candidates are pursued by the ITG, the ITG is guided by established principles that introduce reasonable due diligence, integrity and transparency into the Traceback process. The principles dictate that Tracebacks will be conducted only 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 the ITG staff to be fraudulent, abusive, or unlawful; and
3. Initiation of the Traceback warrants utilization of the ITG's scarce resources.

Prior to initiating a Traceback, the ITG will conduct due diligence to warrant utilization of the Traceback process. Traceback candidates shall be provisioned via the following resources, although the ITG 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 utilize scoring algorithms to identify suspected fraudulent traffic to their subscribers. The ITG may partner with such analytics providers to help identify Traceback candidates.
- ▶ **Enforcement Authorities.** The ITG 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. This cooperation may also include the ITG initiating Tracebacks at the request of appropriate enforcement authorities.

- ▶ **Organizations Subject to Abusive Calling and Scams.** The ITG will partner with private and public organizations to help stop abusive and illegal calls targeting the organizations and their customers. These calls can include robocalls and other spoofed calls targeting an organization's call centers or employees, as well as calls in a Campaign that, without authorization, trade on the brand and reputation of the organization to defraud consumers. The ITG may require a reasonable fee for such Tracebacks.



## **ARTICLE 5: WORKING WITH ENFORCEMENT AGENCIES**

### **Referral to Enforcement Authorities**

In instances where the ITG deems a Voice Service Provider as 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.

In addition, the ITG may refer to appropriate federal and state enforcement authorities information about any originating or intermediate Voice Service Provider that, based on information available to the ITG, fails to effectively mitigate illegal traffic or fails to implement effective measures to prevent new and renewing customers from using its network to originate illegal calls.

When the ITG makes a referral, it will provide a brief written summary of the Traceback investigation(s), which can be in the form of an email communication. The summary will not include any customer proprietary network information (CPNI), but may include the names of Non-Cooperative Voice Service Providers. If an enforcement agency then sends the ITG a subpoena or other lawful request seeking full Incident Data, the ITG will fully comply with those requests.

### **Legal Process/Request for Subscriber Records**

The ITG will not share detailed call records and data with law enforcement without appropriate legal process (e.g., subpoena, Civil Investigative Demand, or other lawful request). The ITG will fully comply with any lawful request. The ITG, however, may share such information without appropriate legal process in an emergency involving danger of death or serious physical injury that requires disclosure without delay. In such cases, the ITG will request appropriate legal process and documentation for its records even after the information has been shared.

### **Enforcement Agency Listserv**

The ITG will maintain and operate an information-sharing resource for federal and state government agencies responsible for enforcement of laws and regulations to prevent illegal robocalls. The listserv will provide participating agencies with information pertaining to active campaigns under investigation by the ITG and serve as a resource to ensure coordination among government agencies.

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.

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)
- ▶ Federal Bureau of Investigation (FBI)
- ▶ Department of Homeland Security (DHS)

It is the responsibility of federal and state government agencies and law enforcement officials to make sure contact information is up to date. Only official government email addresses will be permitted on the listserv.



## **ARTICLE 6: ITG RECORD RETENTION POLICY**

The ITG Record Retention Policy is designed to ensure that Incident Data is 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 Incident Data.

The Retention Policy only applies to Incident Data associated with Traceback investigations initiated through the STP. Under this Retention Policy, Incident Data shall be retained in the STP for a period of no less than two years. 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.



## APPENDIX A: PROVIDER TRACEBACK BEST PRACTICES

1. **Dedicated Point of Contact.** Each 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 the ITG related to Suspicious Traffic as well as a back-up person or internal organization. Each Voice Service Provider will provide the ITG 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. The ITG will make the contact list available to Cooperative Voice Service Providers. The ITG will, upon reasonable request, provide such contact information to enforcement authorities.
2. **Ongoing Coordination.** Through the ITG and specifically the STP, each Voice Service Provider will engage in collective coordination regarding instances of Suspicious Traffic and shall respond to Traceback requests from the ITG. Such coordination will include electronically exchanging information related to Suspicious Traffic and ad hoc follow-up as appropriate.
3. **Prompt Response.** The ITG 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 they have a *bona fide* basis to believe that the traffic is Suspicious Traffic. Each Voice Service Provider should endeavor to initiate investigation of the source of Suspicious Traffic request within four (4) business hours of receiving a request and strive to complete the investigation and return results within 24 hours. 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.
4. **Vet the Identity of Customers.** When signing up new customers, each Voice Service Provider should sufficiently vet the customer in a manner consistent with industry best practices.<sup>5</sup> As part of the vetting process, each Voice Service Provider should collect information such as physical location, contact person(s), state or country of incorporation and, for commercial customers, federal tax ID and the nature of the customer's business. Doing so is necessary to provide a prompt response to Traceback requests and will assist in enforcement efforts.
5. **Mitigate Traffic Source.** If, after investigation, a notified Voice Service Provider learns its own systems and/or end users are generating the Suspicious Traffic, or that it is the POE for such Suspicious Traffic, it should 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 should provide such information to the ITG. 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, all Voice Service Providers should take appropriate steps to eliminate acceptance of abusive, harmful, fraudulent, and otherwise illegal traffic.

6. **Analyze and Monitor Network Traffic.** Each Voice Service Provider should analyze high-volume voice network traffic to identify and monitor patterns consistent with illegal robocalls. For example, each Voice Service Provider should employ tools to detect and act on such patterns.
7. **Investigate and Mitigate Suspicious Calls and Calling Patterns.** If a Voice Service Provider detects a pattern consistent with or specific to illegal robocalls, or if it otherwise has good reason to suspect illegal robocalling or illegal spoofing is taking place over its network, the Voice Service Provider should seek to identify the party that is using its network to originate, route, or terminate these calls and take appropriate action. Appropriate actions may include, but are not limited to, initiating a Traceback investigation; verifying that the originating commercial customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name; reviewing complaints; terminating the party's ability to originate, route, or terminate calls on its network; and notifying law enforcement authorities. Foreign-originating traffic that uses +1 USA Caller-ID values requires special scrutiny.
8. **Privacy of Call Traceback Information.** No Voice Service Provider will share information about a Campaign under investigation provided by another party with any third-party entity except (i) the ITG via the STP, (ii) Voice Service Providers in the call path with the immediate Voice Service Providers to whom they sent or received the call, or (iii) pursuant to a valid legal process, provided however that any individual 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 challenge the legal process. Information gathered by Voice Service Providers during such investigations, including CPNI, shall be used solely for the purpose of conducting Suspicious Traffic investigations and mitigating that Suspicious Traffic. Nothing in this privacy section prohibits a Voice Service Provider from independently disclosing to an enforcement agency information it has obtained outside of the ITG Traceback process, consistent with the law and with its own privacy policy





## APPENDIX B: DO NOT ORIGINATE POLICY

This Do Not Originate Policy outlines the policies and procedures to be utilized by 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, the ITG has instituted DNOs on behalf of government agencies at the federal and state level. To be considered for DNO treatment, a number: (1) must be inbound-only; (2) should be currently spoofed by a robocaller to perpetrate impersonation-focused fraud; (3) must be authorized for participation in the DNO effort by the party to which the telephone number is assigned; and (4) must be recognized by consumers as belonging to a legitimate entity, lending credence to the impersonators and influencing successful execution of the scam. In addition, the number should be the source of a substantial volume of illegal calls.

### DNO Policies for Private Organizations

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

- ▶ **Thorough Vetting.** Both the ITG and ITG Steering Committee Members shall vet the private organization seeking a DNO. Where the private organization 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 organization is a legitimate company active in commerce. Where the private organization is not a customer of an ITG Steering Committee Member, the ITG shall undertake similar vetting. The ITG may accept a DNO from a vendor or other entity on behalf of a private organization, as long as appropriate contractual and administrative protections are in place to ensure valid authorization and sufficient vetting.
- ▶ **Active Event—Volume Thresholds.** A DNO generally shall only be implemented when the private organization is experiencing active and significant fraudulent activity caused by the spoofing of its number. In consultation with the ITG Steering Committee Members, the ITG, however, may initiate a DNO for less significant activity if unique and exigent circumstances warrant such action.
- ▶ **Administrative Charge.** The ITG may charge a recurring administrative fee to any private organization seeking a DNO.

## **Maintaining the Integrity of DNO Implementation**

No less than twice per year, the ITG 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, the ITG may instruct the ITG Steering Committee Members to remove the DNO.

The ITG shall also maintain a registry of all DNOs that have been implemented (whether for private or governmental entities) by the ITG (“DNO Registry”). For each DNO that has been implemented, the 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 the ITG a copy of the DNO Registry. In addition, the ITG at its sole discretion, may share copies of the DNO Registry with analytics providers 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.

## **DNO Implementation is Voluntary and Subject to Provider Discretion**

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 the ITG, the ITG Member shall affirmatively report to ITG staff that the DNO has been implemented, as well as the date of implementation.

Administratively, it may not be feasible for Voice Service Providers to implement DNO for a large group of telephone numbers. Accordingly, in the event the DNO Registry includes more DNOs than a given ITG Member can implement, the ITG Member should implement DNOs as it believes appropriate, prioritizing the DNOs that will most effectively protect its customers. In particular, ITG Members generally should prioritize government-requested DNOs, as well as DNOs associated with high call volume in the areas served by the ITG Member. The ITG may make information available to ITG Members regarding suggested priority DNOs.



## ENDNOTES

- 1 These Policies and Procedures primarily focus on tracebacks, though a related ITG initiative, the Do Not Originate Registry, is addressed in an appendix.
- 2 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).
- 3 See <https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf>. Note: For those Voice Service Providers who offer wholesale voice services but do not offer retail service to end-use customers, 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 a prospective 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 Anti-Robocall Principles.
- 4 Because disclosing customer or call record information to the ITG helps to eliminate illegal calls on a provider’s network, doing so also helps to protect the rights and property of the service providers that share the information
- 5 See Best Practices for the Implementation of Call Authentication Frameworks, NANC Call Authentication Trust Anchor Working Group, sec. 3.1, <https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>.