

**INDUSTRY
TRACEBACK
GROUP**

POLICIES AND PROCEDURES

REVISED AUGUST 2025

INDUSTRY
TRACEBACK◀◀◀
GROUP

INDUSTRY TRACEBACK GROUP OVERVIEW

The Industry Traceback Group (ITG) Policies and Procedures govern the operations of the ITG, outlining criteria for membership and community participation, as well as the management of Traceback and Trace Forward activities, Do Not Originate Registry and other initiatives. These policies ensure that the ITG operates in a neutral, transparent, and competent manner.

The ITG fosters broad cooperation among industry participants in the United States and internationally to enhance trust in voice services and protect users from fraudulent, abusive, and unlawful calls. The primary mission is to identify the sources of such calls and to help ensure their elimination, thereby safeguarding the integrity of voice service networks.¹

TABLE OF CONTENTS

Article I: ITG Structure and Membership	4
Executive Committee.....	4
Steering Committee.....	4
ITG Community (Non-Member Tier)	4
Suspension and Termination.....	5
Article II: Traceback Process	6
Article III: Traceback Sourcing Policy	7
Sources and Principles for Identifying Traceback Candidates.....	7
Article IV: Trace Forward and Emerging Initiatives	9
Article V: Working with Enforcement Agencies	10
Law Enforcement Access to the STP.....	10
Referrals to Enforcement Authorities.....	10
Legal Process for Subscriber Records and Call Path Information.....	10
TRACED Act and Other Reporting Requirements	10
Article VI: Confidentiality, Record Retention, and Publication	11
Confidentiality of Traceback Results.....	11
Record Retention Policy.....	11
Information Sharing and Traceback Information Publication	12
Appendix A: Glossary	13
Appendix B: Provider Traceback Best Practices	16
Appendix C: Do Not Originate (DNO) Policy	18
Overview.....	18
DNO Eligibility and Evaluation Criteria	18
ITG Discretion and Ongoing Review.....	18
DNO Registry	19
Usage and Provider Discretion	19
Access to the ITG DNO Registry.....	19
Contact for Redress	20
Endnotes	21



ARTICLE I: ITG STRUCTURE AND MEMBERSHIP

The Industry Traceback Group (ITG) includes two levels of membership—Executive Committee and Steering Committee—as well as a broader non-member tier known as the ITG Community. While membership provides formal roles in governance and operations, all Voice Service Providers—regardless of membership or Community status—can and are expected or required to cooperate in traceback investigations and help mitigate illegal traffic.

Executive Committee

The Executive Committee is composed of select Steering Committee Members and works closely with ITG staff to shape the ITG's overall strategy and budget. Executive Members provide the bulk of the ITG's membership funding and serve as the primary strategic advisors to the organization.

Steering Committee

Steering Committee Members contribute financial support at a level below that of Executive Members. Admission is at the sole discretion of the ITG and may be based on additional factors, such as the provider's frequent proximity to Originating Providers, U.S. Points of Entry, and/or identified Non-Cooperative Providers in tracebacks.

To qualify for the Steering Committee, a provider must:

1. Be a Cooperative Voice Service Provider with a sustained, active role in the traceback process via the Secure Traceback Platform (STP);
2. Sign a statement of intent to adopt the Best Practices in Appendix B;
3. Affirm commitment by the provider and its affiliates to the State Attorneys General Anti-Robocall Principles.²


Steering Committee Members contribute financial support at a level below that of Executive Members. Admission is at the sole discretion of the ITG and may be based on additional factors, such as the provider's frequent proximity to originating providers, U.S. Points of Entry, and/or identified Non-Cooperative Providers in tracebacks.

ITG Community (Non-Member Tier)

The ITG Community is a non-member tier that allows additional Voice Service Providers to make additional efforts to mitigate unlawful traffic consistent with the ITG's mission and access certain traceback-related resources. To qualify, a Provider must:

1. Complete the onboarding process, which includes submitting information to the ITG;
2. Sign a statement of intent to adopt the Best Practices in Appendix B.

Community Participants will be expected to pay a reasonable fee as part of the onboarding process and for ongoing vetting. Designation as a Community Participant



is at the ITG's sole discretion. Executive and Steering Committee Members are automatically considered part of the Community.

Community participation does not constitute ITG membership or endorsement. Participants may not represent themselves as members or as having been approved, vetted, or certified by the ITG, whether with regard to their robocall mitigation efforts or otherwise. Misrepresentation may result in removal.

Community Participants may be granted access to certain enhanced tools to support mitigation efforts. For example, eligible Participants may receive access to the Traceback Insights Risk Score (see Article VI for more information).

Suspension and Termination

Membership in the ITG and participation in the ITG Community are privileges—not a right—neither ITG membership nor Community participation are necessary to meet any legal or regulatory requirement. ITG Members in particular are expected to serve as models in the fight against illegal calls. Accordingly, the ITG, with the advice of the Executive Committee, may terminate the membership of any Member for cause. Cause includes, but is not limited to, failure to adhere to these Policies and Procedures or repeatedly appearing as the Originating Voice Service Provider or U.S. Point of Entry (POE) in Tracebacks. Prior to termination, the Member will have an opportunity to present to ITG staff and, as appropriate, the Executive Committee, reasons why membership should not be revoked. Termination does not preclude future reinstatement.

In addition, an ITG Member may be suspended if it is named in an enforcement action—such as a formal complaint, Notice of Apparent Liability, or cease-and-desist—or is credibly alleged to have originated or allowed the transmission of illegal robocalls. Suspension does not require any finding by the ITG as to liability or intent. It includes removal from ITG public materials, meetings, and member communications.

While suspension will ordinarily remain in place until the enforcement matter is resolved, the ITG may, with the advice of the Executive Committee, lift or modify the suspension earlier based on the circumstances—including feedback from the provider, the enforcement authority, or other stakeholders. A suspended provider may request reinstatement at any time by presenting reasons to ITG staff, which will seek the advice of the Executive Committee in making a determination on the suspension. If a suspension remains in place for more than one year, the membership will be automatically terminated, unless the ITG, with the advice of the Executive Committee, determines that continued suspension is appropriate under the circumstances. Providers terminated due to the length of suspension may reapply for membership following resolution of the enforcement action.

Community Participants may be removed at the sole discretion of the ITG for any reason, including reputational harm, failure to comply with ITG policies, failure to complete onboarding or participation requirements, or being named in an enforcement action.



ARTICLE II: TRACEBACK PROCESS

The ITG initiates traceback investigations to identify the source of illegal or suspicious voice traffic. Tracebacks proceed through the Call Path until the Originating Provider and end-user caller are identified, regardless of whether the calls originate in the U.S. or abroad, unless impeded by a Non-Cooperative Provider. For foreign-originated calls, the ITG also identifies the point of entry (POE) to the U.S. public switched telephone network. In cases where a call enters and exits the U.S. multiple times, the ITG may identify more than one U.S. POE.

Tracebacks are initiated based on call data from government agencies, industry partners, or analytics providers, as detailed in Article III. The ITG relies on its Secure Traceback Platform (STP) to automate traceback efforts, with providers responding via the STP either manually or automatically through the ITG's API specification.

Upon initiation, the STP notifies the Terminating Voice Service Provider whose customer received the suspicious traffic. Each provider in the Call Path identifies its upstream provider and enters that information into the STP. If an upstream provider is unknown, the downstream provider supplies contact details to update the platform. Providers must maintain accurate, current contact information for their upstream partners. The ITG also collects and incorporates STIR/SHAKEN caller ID authentication data when available and uses the Federal Communications Commission's (FCC) Robocall Mitigation Database to supplement provider information.

The ITG will generally treat as a single Voice Service Provider any entities that directly or indirectly control, are controlled by, or are under common control with one another, unless the provider requests separate treatment or where affiliates are located in foreign jurisdictions.

All Traceback communications—including provider responses and comments—are automatically logged in the STP. If a provider does not respond within the required timeframe, the Traceback may be closed automatically, and the provider may be designated Non-Cooperative. The STP marks Call Path Hops with standardized labels such as No Response, U.S. Origin, International Origin, U.S. Point of Entry, Foreign Point of Departure, and Not Found.

Traceback results are documented in the STP, retained indefinitely, and may be shared with enforcement agencies and other stakeholders consistent with Articles V and VI. Providers failing to cooperate with Traceback requests may be publicly identified as Non-Cooperative per Article VI.

At times, in response to requests from foreign law enforcement, the ITG may trace calls terminating outside the U.S. These are separately categorized within the STP from calls targeting U.S. individuals.

Throughout all Traceback activities, the ITG operates neutrally and non-discriminatorily, consistent with the TRACED Act, ensuring fairness and objectivity in identifying sources of illegal or suspicious traffic.



ARTICLE III: TRACEBACK SOURCING POLICY

This Article outlines the process the ITG uses to identify calls and calling Campaigns selected for Tracebacks. The principal goal is to ensure all Tracebacks initiated by the ITG are done in good faith to identify sources of illegal, fraudulent, or abusive traffic, thereby meeting the requirements of 47 USC § 222(d)(2).

Specifically, the ITG's good faith efforts ensure that Tracebacks are initiated under one of the following conditions:

- ▶ To protect the rights or property of Voice Service Providers,
- ▶ To protect users of voice services and other Voice Service Providers from fraudulent, abusive, or unlawful use of, or subscription to, such services,
- ▶ With the approval of the customer of the voice service receiving suspicious traffic.³


Sources and Principles for Identifying Traceback Candidates

To ensure only actionable Traceback candidates are pursued, the ITG follows principles that introduce reasonable due diligence, integrity, and transparency into the process. Tracebacks will be initiated only if:

- ▶ A credible and verifiable source provides information regarding the candidate,
- ▶ The nature of the traffic is deemed by ITG staff to be fraudulent, abusive, or unlawful, and
- ▶ Initiation appropriately balances the burden on the Voice Service Provider ecosystem and the ITG's internal resources with the expected impact of the Traceback.

Before initiating a Traceback, ITG conducts due diligence to confirm these criteria are met. Candidates are provisioned through the following resources when the criteria are satisfied:

- ▶ **Analytics Providers:** The ITG partners with analytic providers who use scoring algorithms to detect suspected fraudulent traffic.
- ▶ **Enforcement Authorities:** The ITG cooperates with requests from local, state, and federal enforcement authorities to provide actionable leads on active suspicious traffic and may initiate Tracebacks at their request. The ITG may also receive requests, including from foreign law enforcement, to trace calls received outside the United States. Tracebacks conducted in response to these requests are categorized separately within the STP.
- ▶ **ITG Steering Committee Members and Community Participant Referrals:** Steering Committee Members may identify candidates and use good faith efforts to ensure their validity. Community participants may submit referrals, which the ITG reviews for potential Traceback initiation on a case-by-case basis.
- ▶ **Organizations Subject to Abusive Calling and Scams:** The ITG collaborates with private and public organizations on Traceback requests to combat abusive or illegal calls targeting the organizations and their customers or clients. This includes



robocalls, spoofed calls targeting call centers or employees thereof, and unauthorized campaigns that trade on an organization's brand to defraud consumers. The ITG may require a reasonable fee for Tracebacks requested under this category.



ARTICLE IV: TRACE FORWARD AND EMERGING INITIATIVES

The ITG continually adapts its operations to meet the evolving challenges posed by illegal and abusive calling, while maintaining predictability and fairness for Voice Service Providers.

For example, the ITG conducts Trace Forwards, a process to determine the ultimate destination and recipient of a call returned to a callback number used in an illegal calling scheme, such as those included in smishing (SMS-based phishing) attempts. Rather than tracing the original call, the ITG follows the call-back path by contacting Voice Service Providers that serve the call-back number and requesting information about the associated customer. The process continues provider by provider until the responsible party is identified or no further information is available. These investigations are conducted via the STP and help identify downstream recipients that may be involved in, or impacted by, a broader call campaign.

The ITG has launched new pilot initiatives to support investigatory or illegal call disruption efforts and may do so in the future. Pilot initiatives will generally rely on the cooperation of Voice Service Providers committed to stopping illegal call campaigns and may inform broader operational strategies for the ITG, enforcement coordination and referrals, and/or STP development.



ARTICLE V: WORKING WITH ENFORCEMENT AGENCIES

Law Enforcement Access to the STP

The ITG maintains and operates secure access to the STP for federal and state government agencies responsible for enforcing laws and regulations intended to prevent illegal calls. This access provides participating agencies with timely information about active campaigns under ITG investigation and serves as a resource to facilitate coordination among enforcement entities.

Access is limited to federal and state government agencies actively engaged in investigating illegal and fraudulent calls. Eligible agencies include, but are not limited to, the Federal Communications Commission, Federal Trade Commission, Social Security Administration, State Attorneys General, Treasury Inspector General for Tax Administration, Federal Bureau of Investigation, and Department of Homeland Security. It is the responsibility of participating agencies to maintain current contact information, and only official government email addresses are permitted for STP access.

Referrals to Enforcement Authorities

In addition to providing information through STP access, the ITG may refer to appropriate enforcement authorities any Voice Service Provider whose conduct raises concerns, including but not limited to deliberate provision of false or misleading information to the ITG, failure to respond or cooperate in Traceback efforts, or apparent violations of FCC call authentication and Robocall Mitigation rules.

When making referrals, the ITG will provide a summary of relevant investigation findings. This summary will exclude customer proprietary network information (CPNI) but may identify relevant Voice Service Providers.

Legal Process for Subscriber Records and Call Path Information

The ITG will not release detailed call records or subscriber data or full Call Path information to law enforcement without appropriate legal process such as subpoenas or civil investigative demands. The ITG will comply fully with lawful requests, including subpoenas, for detailed Traceback and Incident Data. Exceptions are made only in emergency situations involving imminent risk of death or serious injury, where disclosure may proceed prior to formal legal process, with subsequent documentation expected.

TRACED Act and Other Reporting Requirements

The ITG cooperates with lawful requests from the FCC to disclose certain data about Traceback participants pursuant to the TRACED Act. For example, in the annual TRACED Act report, the FCC requests and publishes information about participating and Non-Responsive Providers.



ARTICLE VI: CONFIDENTIALITY, RECORD RETENTION, AND PUBLICATION

Confidentiality of Traceback Results

Although the ITG exclusively traces suspected illegal calls, data acquired through these investigations reveals business relationships among providers and may include end user information that is subject to privacy protections. The ITG treats this information as confidential due to both privacy and competitive concerns.

Accordingly, the ITG limits the data it shares and makes publicly available. In the STP, providers are not privy to the full Traceback, i.e., all information collected about every Hop in the Call Path. However, some data regarding an upstream provider's role—such as whether the upstream provider originated the traffic or was downstream of a Non-Responsive Provider—may be shared for awareness and accountability.

In the case of Tracebacks initiated at the request of a private organization, the ITG shares information about the caller and Originating Provider sufficient to support the organization's efforts to investigate and mitigate harmful traffic. The ITG will disclose additional Call Path details only when necessary, as determined exclusively by the ITG. Such disclosures are limited to stopping the abusive campaign or protecting the organization and its customers. Recipients may use and share such information only for the purpose of stopping the harmful traffic, including, as appropriate, making referrals to law enforcement agencies.

Sharing of Traceback-related information with federal and state enforcement authorities is governed by Article V.

Record Retention Policy

The ITG Record Retention Policy is designed to balance the need to maintain data that may assist federal and state enforcement agencies with future investigations and enforcement actions, and support ITG efforts to promote accountability and mitigate illegal calls, while practicing data minimization to enhance security, privacy, and efficient data store.

Under this policy, the ITG retains all Incident Data and any other data obtained through Tracebacks indefinitely. However, for Incident Data not used in Tracebacks, the ITG obfuscates the terminating number and purges any associated voicemails. Where Incident Data has been used in a Traceback, it is retained in full as part of the official Traceback record.

While this policy currently provides for indefinite retention, the ITG may revisit and revise this timeline in the future if evolving security, privacy, or data storage considerations warrant a shorter retention period.

Voice Service Providers that participate in Tracebacks may also maintain their own internal data retention policies.

For purposes of this policy, “retain” refers to the storage or maintenance of relevant records in any format.



Information Sharing and Traceback Information Publication

The ITG reserves the right to publish the identity and status of Non-Cooperative Voice Service Providers. Such information may be made available to ITG Members or Community Participants, or published through the STP, the ITG website, email communications, periodic reports, or other formats.

The ITG also makes available to participating Voice Service Providers information about providers that do not cooperate or that, based on available data, appear to be in blatant violation of FCC rules—such as those governing submissions to the Robocall Mitigation Database. Any provider publicly designated as Non-Cooperative may be removed from such listings if they later demonstrate they no longer meet the definition of Non-Cooperative.

The ITG maintains a Traceback Insights Risk Score, a proprietary indicator derived from patterns in Traceback data and provider behavior. This score helps assess provider risk based on Traceback history. Providers have access to their own Traceback Insights Risk Score and Members of the ITG Community may, subject to appropriate usage and access controls, access Traceback Insights about other providers to support their Know Your Upstream Provider obligations and related mitigation and compliance efforts. The Traceback Insights Risk Score reflects patterns observed in Traceback data but does not, on its own, imply complicity, intent, or negligence. It should be interpreted in context alongside other relevant information.

Government agencies may publish data submitted by the ITG as part of the ITG's obligations as the FCC's registered Traceback consortium. For example, the FCC publishes annual TRACED Act reports that include information about participating Voice Service Providers and Non-Responsive Providers, as described in Article V. The ITG may also release aggregate, anonymized metrics or summaries of Traceback activity to inform industry stakeholders, the public, and policymakers.

Nothing in this Article limits the ability of Voice Service Providers to share their own data, outside of the Traceback process, in accordance with applicable law and contractual obligations.



APPENDIX A: GLOSSARY

This glossary includes terms used throughout the ITG Policies and Procedures, as well as additional terms used in ITG operations and in the STP. Some defined terms may not appear in this document but are included to support consistent understanding across ITG activities and materials.

Basis for Traceback: The specific reason or reasons that inform ITG's reasonable suspicion that a call subject to a Traceback is fraudulent, abusive, or unlawful. The basis may be due to information obtained from analytics providers, government agencies, impacted organizations, or other credible sources.

Call Path: The full Hop-by-Hop path that traverses Voice Service Providers' networks from an Originating Provider to a Terminating provider, including all Transit/Intermediate providers.

Campaign: A group of potentially hundreds of thousands or more calls with identical or nearly identical messaging, as determined by the content and calling patterns of the calls.

Campaign Label: An umbrella description for different Campaigns that are grouped by similar characteristics.

Cooperative Voice Service Provider: A Voice Service Provider committed to protecting networks and consumers from fraudulent and abusive robocall traffic by agreeing to, and abiding by, the policies and procedures set forth in this document as well as applicable laws and regulations governing the origination, termination, or transit of voice traffic.


Dispute: A formal challenge submitted by a provider through the STP in response to the basis of a Traceback. All disputes are reviewed by the ITG team and related records and communications are retained as part of the Traceback record, regardless of the outcome.

Downstream Provider: A Voice Service Provider that receives voice traffic from an upstream provider in the Call Path. In the context of ITG Traceback investigations, each provider in a Call Path serves as a Downstream Provider to its immediate Upstream Provider.

Foreign Point of Departure: The Voice Service Provider that immediately precedes a U.S. POE in the Call Path. The ITG primarily relies on the FCC's Robocall Mitigation Database to determine whether a Voice Service Provider is foreign or based in the U.S.

Hop: Each step where a voice call is passed from one provider to another.

Incident Data: Call detail information related to Suspicious Traffic shared by or with the ITG, which can include, but is not limited to: originating and terminating telephone numbers; IP addresses or signaling point codes; Session Initiation Protocol (SIP) header anomalies; STIR/SHAKEN authentication data; call volume and certain call detail record (CDR) data; timestamps; a voicemail or transcript associated with the Campaign; the Basis for Traceback and any other evidence indicating that the traffic may be fraudulent, abusive, or unlawful.



Non-Cooperative Voice Service Provider: A Voice Service Provider that fails to cooperate with the ITG in Traceback investigations, including by failing to respond to a Traceback request in a timely or complete manner or failing to take appropriate mitigation steps in ways that such conduct materially impairs the effectiveness of Traceback operations.

Non-Responsive Voice Service Provider: A Voice Service Provider that fails to respond in a timely manner to a Traceback request, explicitly refuses to cooperate with a Traceback, or submits false or misleading information. All Non-Responsive Voice Service Providers are considered Non-Cooperative Voice Service Providers.

Not Found: A Hop found in the Call Path of a Traceback where a provider cannot locate the call or where a call is incorrectly identified in the Call Path.

Originating Provider: The Voice Service Provider identified by the ITG as the entity that enabled a calling party to use its network to originate calls later deemed illegal or abusive.

Secure Traceback Platform (STP): The online platform managed by the ITG to facilitate Tracebacks and identify Originating Voice Service Providers responsible for suspicious or illegal call traffic.

Strike Exempt: A Traceback which the ITG determines is unreliable —due to, for example, factual issues, technical errors, testing, or an accepted Dispute. Strike Exempt Tracebacks are not counted in aggregate metrics but may still be shared with government authorities pursuant to a subpoena. In such cases, the submission will indicate that the Traceback was marked Strike Exempt and explain why.


Suspicious Traffic: One or more voice calls suspected of being abusive, unlawful, or fraudulent based on indicators that may include, but not limited to: complaints or referrals from consumers, law enforcement, or third parties regarding unauthorized spoofing; unlawful content in transcripts or recordings of the calls; unusual call volumes or patterns; missing or altered call information; or other evidence suggesting the traffic may harm consumers, violate applicable laws or regulations, or undermine network integrity.

60-Day Status: An objective assessment of a provider's involvement in Tracebacks over the past 60 days displayed in the STP as a yellow or orange flag. 60-Day Status is separate from the Traceback Insights Risk Score.

Terminating Provider: The Voice Service Provider who provides service to the end user or customer that received the suspected unlawful calls subject to a traceback. The Terminating Provider is the starting point and first Hop of a Traceback investigation.

Traceback: A network-based process to identify the source of Suspicious Traffic beginning with a terminating Voice Service Provider and proceeding upstream through the Call Path to the Originating Voice Service Provider and/or a Non-Cooperative Provider.

Traceback Insights Risk Score: A numerical risk indicator developed by the ITG assessing a provider's Traceback history relative to other providers. The score reflects patterns observed in Traceback data but does not, on its own, imply complicity, intent, or negligence. It should be interpreted in context alongside other relevant information.



Trace Forward: A process using the STP to follow the downstream Voice Service Providers in the Call Path to identify the party that receives a call at a call-back number, such as an entity behind a scam that prompts victims to return a call in smishing or voicemail baiting attacks.

Transit/Intermediate Provider: A Voice Service Provider in the Call Path between the Terminating Provider and the last identified provider, which may be the Originating Provider or a provider in the Call Path that does not cooperate with the traceback request.

Upstream Provider: A Voice Service Provider that delivers call traffic to another Voice Service Provider. In any given Traceback or Call Path, the Upstream Provider may be a Transit/Intermediate provider or could be the Originating Provider.

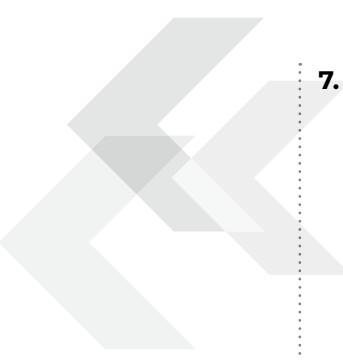
U.S. Point of Entry (POE): A Voice Service Provider within the U.S. Call Path who accepts a call from a foreign Voice Service Provider. In cases where a call enters and exits the U.S. multiple times, there may be more than one U.S. POE.

Voice Service Provider: A provider of any voice service, interconnected with the public switched telephone network (PSTN) that furnishes communications to an end user. A Voice Service Provider may be U.S.-based or foreign. The ITG will generally treat as a single Voice Service Provider any entities that directly or indirectly control, are controlled by, or are under common control with one another, unless the provider requests separate treatment or where affiliates are located in foreign jurisdictions.⁴



APPENDIX B: 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 informal requests from other Cooperative Voice Service Providers or request from 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, upon reasonable request, provide such contact information to enforcement authorities.
- 2. Ongoing Coordination.** Through the ITG and specifically through the STP, each Voice Service Provider will engage in informal collective coordination regarding instances of Suspicious Traffic and in addition to shall respond to Traceback requests from the ITG. Such coordination may 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 complete the investigation and return results within 24 hours per FCC rules. 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.⁵ 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 Voice Service Provider is notified that its systems and/or end users are generating Suspicious Traffic, or that it is a POE for Suspicious Traffic, it should take steps to investigate and mitigate the Suspicious Traffic. If a Traceback investigation results in a finding that the traffic was lawfully originated, the Voice Service Provider originating the lawful traffic should provide this information to the ITG. To ensure that consumers, businesses, and Voice Service Providers are protected from illegal calls 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 voice network traffic to identify and monitor patterns consistent with illegal calls. For example, each Voice Service Provider should employ tools to detect and act on such patterns. Foreign-originating traffic that uses +1 USA Caller-ID values requires special scrutiny.

- 
- 7. Investigate and Mitigate Suspicious Calls and Calling Patterns.** If a Voice Service Provider detects a pattern consistent with or specific to illegal calls, or if it otherwise has good reason to suspect illegal calling 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.
- 8. Privacy of Call Traceback Information.** No Voice Service Provider will share information provided by another party about a Campaign under investigation with any third-party entity except (i) the ITG via the STP, (ii) the immediate Voice Service Providers to whom they sent or from whom they 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 C: DO NOT ORIGINATE (DNO) POLICY

Overview

This Do Not Originate Policy outlines the procedures used by the ITG to implement DNO requests. DNO is a process whereby certain telephone numbers are identified at VoIP gateways or interconnection points to block calls using those numbers from further transmission. Entities for which a DNO has been instituted are referred to as DNO Recipients. The ITG maintains a DNO Registry of numbers for which it received and approved a DNO request.

DNO Eligibility and Evaluation Criteria

The ITG may institute DNOs and add a telephone number to its DNO Registry on behalf of federal or state government agencies or private organizations. To qualify, a number must:

1. Be inbound-only;
2. Be currently spoofed by bad actors to perpetrate impersonation-based fraud;
3. Be authorized for participation in the DNO program by the number's assigned holder; and
4. Be recognizable by consumers as tied to a legitimate entity, increasing the scam's perceived authenticity.

Additionally, the number should be tied to substantial volumes of illegal traffic. In exceptional circumstances, the ITG may approve a DNO request with lesser activity if exigent risk exists. The ITG may, in its sole discretion, apply higher standards for private entities than for governmental bodies.

For private organizations:

- ▶ The ITG will vet private requesters and may accept third-party submissions if sufficient contractual and administrative protections are in place.
- ▶ If the organization is a customer of an ITG Executive Committee or ITG Steering Committee Member, the member must verify number ownership.

ITG Discretion and Ongoing Review

The ITG reserves the right to accept, reject, or remove DNO entries from its Registry at its sole discretion based on operational considerations, threat intelligence, or other relevant factors.

- ▶ The ITG will confirm at least biannually with each DNO Recipient that the conditions supporting their DNO designation remain valid (e.g., number is still inbound-only and still assigned to the recipient).
- ▶ Without confirmation, the ITG may instruct recipients of the ITG DNO Registry to remove the DNO entry.



DNO Registry

The ITG will maintain a registry (“DNO Registry”) that includes:

1. Name of the DNO recipient;
2. Number(s) covered;
3. Date of authorization;
4. Names of Steering Committee Members who implemented the DNO; and
5. Implementation dates.

The ITG may share the registry with:

- ▶ Participating Voice Service Providers (who cooperate with ITG Tracebacks and serve U.S. subscribers);
- ▶ Analytics providers, at its discretion and potentially at additional cost.

Usage and Provider Discretion

- ▶ Usage of the ITG DNO Registry is voluntary for ITG Members. However, the FCC requires all Voice service providers to screen calls against a reasonable DNO list. While the ITG believes its list is reasonable, it does not represent or warrant that it satisfies the FCC’s requirement.
- ▶ Prior to using the ITG DNO Registry, the provider must report confirmation and date to ITG staff.
- ▶ If the volume of DNOs exceeds a provider’s technical ability the provider may select those numbers with the highest protective value. In doing so, providers should consider prioritizing:
 - Government-issued DNOs
 - High-volume spoofed numbers relevant to their customer base

Access to the ITG DNO Registry

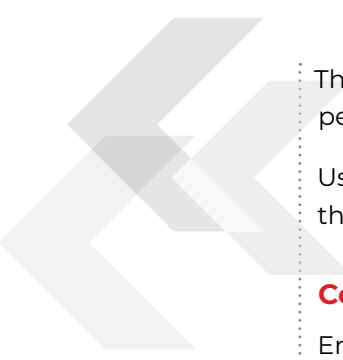
Access to the ITG DNO Registry is governed by the [ITG DNO Registry Terms and Conditions](#), which are incorporated by reference into this Policy. Entities seeking access must agree to those terms, including any updates published from time to time.

Access is limited to eligible Voice service providers that transmit calls to U.S. subscribers and cooperate with ITG Traceback requests. Use of the DNO List is permitted solely to prevent illegal call traffic. Redistribution or use for any other purpose is prohibited.

The DNO Registry includes only numbers for which the subscriber has specifically requested blocking. It does not include invalid, unallocated, or unassigned numbers.

The ITG disclaims all liability for any direct or indirect consequences of usage of its DNO Registry by third parties. Use is at the provider’s sole discretion and risk.

The ITG may charge a reasonable subscription fee for access. Continued access is contingent on timely payment. Failure to pay may result in immediate termination of access, and all copies of the DNO Registry must be deleted.



The DNO Registry is updated as new entries are approved and may be refreshed on a periodic basis. Authorized users will receive instructions for accessing updated versions.

Use of the DNO Registry does not imply endorsement, membership, or affiliation with the ITG.

Contact for Redress

Entities that believe a number has been incorrectly included in the DNO Registry may contact the ITG at legal@tracebacks.org.



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 See [State Attorneys General Anti-Robocall Principles](#). 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.
- 3 Disclosing customer or call record information to the ITG helps to eliminate illegal calls on a provider's network and helps to protect the rights and property of the service providers that share the information.
- 4 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).
- 5 See Best Practices for the Implementation of Call Authentication Frameworks, NANC Call Authentication Trust Anchor Working Group, sec. 3.1, [FCC Document](#).