ZipDX®

27 May 2021

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

RE: Letter of Intent to serve as the Registered Industry Consortium (EB 20-22, DA 21-474)

Dear Ms. Dortch,

As the leading advocate for traceback, both in words and action, ZipDX LLC is pleased to respond to the Enforcement Bureau's request for letters of intent to become the registered industry consortium for tracebacks (DA 21-474, released April 26, 2021). Below we present:

- An overview of this submission
- A review of the increasingly critical role of traceback in robocall mitigation efforts
- Our view of the priorities for traceback given the stakeholders it serves
- The history of traceback and the key role that ZipDX has played
- Details for certain elements of the Best Practices we adopt
- Our long-standing record of traceback innovation and thought leadership
- Factors buttressing our organization's technical superiority
- A formal statement of our compliance with the requirements of the TRACED Act and the Commission's rules – specifically, sections 13(d)(1)(A) through D of the Act and §64.1203 (b) of the Commission's rules

Overview

Eight years after ZipDX first defined an automated system for traceback, it is now routine, with hundreds of organizations and their teams – including the Commission, USTelecom, providers, analytics companies and enforcers – contributing to its success.

But the job clearly is not done; the robocall scourge continues.[1] We have not delivered to Americans the relief they demand; we have not taken back our Public Telephone Network

[1] See YouMail's Robocall index at https://robocallindex.com/, showing a general ongoing upward trend in robocall volume. Also see May 24 and May 27 comments in the Wall Street Journal: https://www.wsj.com/articles/scammers-and-fraudsters-from-sea-to-shining-sea-11621804820?st=bh5df33px6gyc0a&reflink=desktopwebshare_permalink; https://www.wsj.com/articles/its-time-to-finally-crush-spam-phone-calls-11622057098?st=w6e0wgj7q5brdkg&reflink=desktopwebshare_permalink

from the lawbreakers that have ruined the phone call experience. Traceback today can find and shut down bad actors one at a time, but the calls persist as new perpetrators appear.

Getting ahead of this cycle requires a better integration of efforts by service providers and enforcers, incorporating new tools along the way. Identifying unlawful campaigns, sourcing associated call examples, identifying the source, and informing the responsible parties (plus enforcers if required) are the fundamental elements of effective mitigation.

- STIR/SHAKEN identifies the signer of a call, but extracting and acting on information from the associated IDENTITY header must be integrated into existing notification and enforcement processes to take advantage of that new technology.
- Similarly, the call path from traceback has to be vetted against the Commission's new Robocall Mitigation Database (RMD) as part of leveraging that resource.

These and other enhancements are necessary to make traceback better and faster and more effective, which are paramount in moving away from whack-a-mole to the point that unlawful calls slow to a trickle.

We will not get there with a steady-as-she-goes approach to traceback. Traceback needs continuous innovation. It needs a steward that is creative, nimble and dynamic, with deep technical knowledge and operational expertise.

ZipDX is uniquely qualified to be the registered consortium for traceback. Our extensive record is distinguished not just by our thought leadership and operational accomplishments, but also by our established history of innovation and responsiveness. We developed and ran the automatic traceback system under the USTelecom banner.[2] Selecting ZipDX is not a bet on a newcomer – it is a mandate to us to redouble our effort and take traceback to the necessary next level.

As we enter this next phase, Americans need everything they can get from traceback. Maintaining the status quo will not be good enough. With our passion, expertise, and laser focus, traceback will be optimized and updated to deliver maximum value to all stakeholders.

The Critical Role of Traceback

In 2013, ZipDX first detailed the traceback concept in the context of robocall mitigation. In our submission to the Federal Trade Commission's Robocall Challenge, we explained:

[2] See page 7 for additional detail on our work with USTelecom.

Carriers are the guardians of the United States PSTN. Responsible Carriers make it their business to insure that the network operates reliably and efficiently, and that the traffic on the network is lawful. All traffic comes into the PSTN via a Carrier. Sometimes there are other "service providers" in front of the Ingress Carrier; for example, some VoIP providers aggregate traffic from many customers and then pass that traffic to a partner Carrier to put it on the PSTN. International traffic comes in legacy or VoIP format from an overseas provider and enters the US PSTN through a US Carrier. In these cases there is always a business arrangement (typically a contract) between the originating provider and the Carrier.[3]

Since that submission, ZipDX has relentlessly advocated for traceback. As stakeholders began to understand our thesis, it set the stage for a fundamental shift in accountability for illegal robocalls. Heretofore, providers merely passed through the calls they received. Complicit providers were earning a fee for putting illegal calls onto the network; some were even soliciting such traffic. Recognizing this, regulators and legislators, with industry support, moved to put affirmative obligations on providers to reject such calls.

The ability to find the specific providers enabling the illegal callers was key. Our submission detailed the traceback process, starting with a consumer complaint or machine-captured illegal call example. Such an event would trigger an automated traceback sequence from the terminating provider to the point where the call entered the network. We wrote: *Our intention is that the above process is fully automated and the data retrieved in seconds. To the extent that technical barriers prevent us from achieving that goal initially, we will employ semi-automated techniques (such as automatically dispatching secure emails to designated contacts at participating carriers, requesting manual call traces with automatic parsing of the returned results). This will allow us to grow into the large volume of transactions that will ultimately be required.*[4]

Those explanations from eight years ago describe how traceback functions today. It works so well that it has been codified in law; the TRACED Act dictates this proceeding to designate a registered consortium to perform the function. The Commission's Fourth Report and Order in Docket 17-59, addressing Advanced Methods to Target and Eliminate Unlawful Robocalls[5], mandates cooperation with the traceback process and holds originating providers accountable for the traffic they accept. The Commission's Second Report and Order in WC Docket No. 17-97, regarding the Call Authentication Trust Anchor

[3] "It's My Number" from ZipDX, page 8. Our submission is archived at this Federal Trade Commission web location: https://www.ftc.gov/sites/default/files/documents/public_comments/2013/05/565017-00023-85936.pdf.
[4] Ibid, page 6. Additional step-by-step detail is in the document at page 5.
[5] https://docs.fcc.gov/public/attachments/FCC-20-187A1.pdf

(implementing STIR/SHAKEN)[6], invokes traceback as a key pillar: the fallback mitigation tool to be employed when providers are granted an extension, use legacy networks, or opt not to authenticate calls they receive in their role as an intermediate provider, is traceback. Traceback results have been strategic for FCC enforcement actions (including the largest fine ever levied[7]) and are part of the Enforcement Bureau's on-going efforts to rein in complicit providers, with two new cease-and-desist letters[8] this month.

Beyond the FCC's embrace of traceback, it has been a key element in enforcement actions by other agencies. The Department of Justice, Federal Trade Commission, Social Security Administration, along with several state Attorneys General and other agencies have leveraged it. In numerous cases, settlement agreements dictate on-going adherence to metrics built on traceback.

Given this backdrop, it is clear that traceback must continue to evolve. With so much riding on it, the registered consortium must be held to the highest standard. This is why Congress specified explicitly that the Commission revisit the registration selection annually (not 3 years or some other interval as used elsewhere in the Act)[9].

Expanding on this, the Commission wrote in its Order implementing this selection process: *An entity that seeks to become the registered consortium must sufficiently and meaningfully fulfill the statutory requirements.* ***Based on our experience, we expect the traceback process to evolve in response to new unlawful robocalling schemes, new technologies, and the needs of interested parties, such as the Commission, the Department of Justice, state Attorneys General, and other agencies.*** *Accordingly, we wish to encourage, not hinder, a responsive, dynamic traceback process. We must, however, ensure that the registered consortium is accountable for compliance with the statutory requirements. We will set forth a set of principles, rather than prescriptive directives, for the Bureau to use to select the registered consortium and ensure that it complies with section 13(d)(1)(A)-(D) of the TRACED Act.* ***This approach will ensure a reasonable balance between ensuring statutory compliance with the need for a nimble and dynamic traceback process***.[10] (emphasis added)

Given the growing role that traceback plays, it is critical that the selected Registrant, having passed the statutory compliance requirements, possess the vision, the domain knowledge,

[6] https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf
[7] https://www.fcc.gov/document/fcc-issues-record-225-million-fine-spoofed-robocalls
[8] https://www.fcc.gov/document/fcc-demands-two-companies-cease-and-desist-illegal-robocall-campaigns
[9] See TRACED Act Section 13 (d) (2); contrast, for example, with Section 4 (b) (4) regarding call authentication
[10] FCC EB Docket No. 20-22, Implementing Section 13(d) of the TRACED Act, paragraph 15 (https://docs.fcc.gov/public/attachments/FCC-20-34A1.pdf)

and the technical know-how to support the demands of an expanding cadre of stakeholders, supported by the strongest proven track record.

Traceback Priorities & Stakeholders

The registered consortium has no enforcement authority; its objectives are to:

- Gather information about fraudulent, abusive or unlawful traffic.
- Make that information actionable by:
    - Correlating it with other data
    - Automatically generating insights from multiple events
    - Sharing it with provider(s) responsible for the call(s) so that they can take effective mitigation steps
    - Providing contextual and detailed reports to enforcement agencies.
- At all times, ensure that any data sharing is well within legal boundaries and does not compromise enforcement efforts.

There are many stakeholders in the traceback process:

- Providers are key to the success of traceback. Responding to traceback requests is required by regulation, but we must not take for granted the resources required to generate those responses. We strive to continuously reduce that burden and make the process as streamlined as possible, for providers large and small.
- Enforcers and regulators depend on the traceback process. We similarly need to enable them to be maximally efficient, through reporting tools and other enhancements that are optimized around their workflow.
- The biggest enemy of lawful callers is the cadre of misfits that pollute the telephone network with illegal traffic. While as Registrant we are not responsible for labeling and blocking of calls, we can work with lawful callers to help industry distinguish the good from the bad.
- Institutions suffer impersonation by fraud callers (Internal Revenue Service, Social Security Administration, utilities, service providers, retailers, etc.). We need to use our tools and our expertise to mitigate abuse of their names and reputations.
- All Americans want their telephone network back from the illegal mass callers holding it hostage. While we do not answer to them directly, they are our ultimate customer.

As the registered consortium, we will work within the Policies and Procedures framework to set priorities that deliver the biggest stakeholder benefits given the available resources. We believe that innovation and automation generally have the highest returns, because after the initial investment, recurring costs are negligible.

ZipDX Traceback Timeline

ZipDX is uniquely suited to anticipate, define, and deliver the innovations needed in traceback. This is evidenced by our extensive history in this space.

2013: In its Robocall Challenge entry, ZipDX outlines the concept of traceback, details how it can be implemented, and lays out the benefits.

2014: ZipDX reiterates its advocacy for call tracing as a tool in the Rural Call Completion context.[11] In this case, the calls would be traced forward, from the point of origination to the point in the network where they failed.

2015: In response to FCC Public Notice DA 14-1700, "Consumer and Governmental Affairs Bureau Seeks Comment on Robocalls and Call-Blocking Issues Raised by the National Association of Attorneys General on Behalf of Thirty-Nine Attorneys General" (WC Docket 07-135 & CG Docket 02-278), ZipDX explains how traceback offers better return on investment than alternatives. We wrote: *Instead of agonizing over approaches that will ultimately fail, carriers, regulators and AGs should be looking for solutions that can track calls to their source(s) and stop them*.[12] ZipDX continued its advocacy in other venues, including a presentation to ATIS, and another at the Voice Telephone Abuse Special Interest Group of the Messaging Malware Mobile Anti-Abuse Working Group (VTA-SIG/M3AAWG).

2016: Regulators and industry start to warm to the notion of rapid traceback, presumably partly in response to our advocacy. It is mentioned briefly in the Robocall Strike Force Report.[13] USTelecom is designated by the Strike Force to lead traceback efforts and, to its credit and thanks to its persistence, over time corrals an initial group of providers to participate in its Industry Traceback Group.

2017: ZipDX files extensive comments in the Commission's ongoing docket in the matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, writing: *Originating providers – that is, that part of the telecommunications industry that places calls onto the United States public switched telephone network as a service to end-users – are ideally positioned to do this and we make explicit recommendations for how to engage them in*

---

[11] ZipDX comments filed April 2, 2014 in WC Docket 13-39, Rural Call Completion NPRM, available at https://ecfsapi.fcc.gov/file/7521096627.pdf

[12] See comments of ZipDX, January 21, 2015, available at https://ecfsapi.fcc.gov/file/60001015739.pdf. Also see our February 21, 2015 ex parte presentation to CGB staff: https://ecfsapi.fcc.gov/file/60001032296.pdf

[13] Robocall Strike Force Report, October 26, 2016, sections 3.1.2 and 3.2.2. Available at https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf.

doing so. Traceback – the process of following a robocall from the call recipient backwards through the network to its source – is a critical element of successful mitigation efforts.[14]

2018: ZipDX explains and promotes traceback to an organization of lawful callers, the Professional Association for Customer Engagement (PACE). Like the rest of us, members of this group are harmed by the scourge of illegal callers. In parallel, in an effort ZipDX dubbed the Robocall Alliance, we attempt to rally industry leaders around investment in technology to accelerate and scale traceback through automation. Frustrated by endless worrying about what might go wrong, the ZipDX team independently develops its Secure Traceback Portal and makes it available to USTelecom's ITG. The first few tracebacks are initiated in December.

2019: The ZipDX Secure Traceback Portal, operating under the auspices of the ITG, hits its stride. The ITG's completely manual original system, based on a mailing list of participating providers, had been processing a handful of tracebacks each month. By May, the ZipDX portal was consistently processing over a hundred, with many completing in a day. ZipDX initiated and sponsored a relationship with YouMail, a consumer-facing robocall mitigation solution employing sophisticated analytics, to provide for traceback consistent, documented examples of unlawful robocalls. ZipDX not only hosted and supported the web-based Portal, but also took on some operational responsibilities for the overall process, including interfacing with providers and enforcers – all without compensation.

2020: At the beginning of the year, Jonathan Spalter, USTelecom's CEO, writes in his 2019 Progress report: *I would like in particular to acknowledge ZipDX, a provider of specialized telecom applications and a longtime advocate of the traceback process.* ***On its own initiative ZipDX developed and made available at no charge to the ITG a web-based traceback system bringing automation and scale to our efforts, while also contributing process innovations and operational expertise.*** *Together, we've evolved traceback into a critical pillar in the fight against illegal robocalls. As a result, we are now routinely — and rapidly — tracing back representative call examples from the most egregious illegal calling campaigns so that they can be stopped at the source.*[15] (emphasis added) ZipDX continues to provide its Secure Traceback Portal through July, when USTelecom replaces it with a separately-developed version based on the original ZipDX architecture. Between December 2018 and July 2020, the original ZipDX Portal initiated over 2,800 tracebacks; the number of participating providers grew by an order of magnitude; and the Portal never went offline. Portal availability is critical, given that CGB's Fourth Report and Order states: *We generally expect*

[14] Comments of ZipDX, June 27, 2017, filed in docket CG 17-59, available at https://ecfsapi.fcc.gov/file/10627304016463/ZipDX-17-59-NPRM-NOI-Comments.pdf

[15] USTelecom Industry Traceback Group 2019 Progress Report, page 2. Available at https://www.ustelecom.org/wp-content/uploads/2020/01/USTelecom_ITG_2019_Progress_Report.pdf

responses within a few hours, and certainly in less than 24 hours absent extenuating circumstances.[16] That can't happen if the platform is not available.

2021: Through the first quarter, ZipDX continues to support the ITG with provider outreach and reports for enforcers and regulators.

Our history demonstrates a relentless drive to address the illegal robocall problem leveraging traceback as part of the solution. The breadth of our interactions shows how deeply we are embedded across the spectrum of stakeholders. But actions speak even louder than words. Beyond just talking, ZipDX is constructively building and deploying solutions.

ZipDX Adopts ITG Policies and Procedures

To avoid any disruption to the traceback process, ZipDX will adopt the current ITG Policies and Procedures as our written best practices. ZipDX is quite familiar with these practices, as we contributed to their development and followed them during our tenure operating our Secure Traceback Portal on behalf of USTelecom.

Structure and Membership: These Policies and Procedures reference an Executive Committee and a Steering Committee, as well as Affiliate Members. ZipDX will maintain the composition of these groups when we launch our operation of the traceback process. We have a history of working with this structure. We initiated and sustained the drafting of monthly reports and participated in regular conference calls with Committee members.

The Policies and Procedures indicate that select Committee members financially support the ITG. We are comfortable continuing this structure. Through our extensive experience with traceback operations, we are familiar with the associated expenses.

Traceback Process: This is now well-established, thanks in large part to the ZipDX Secure Traceback Portal, which mechanized and standardized the process. Most communications are automated with carefully crafted messaging.

We recognize the importance of confidentiality. This was a fundamental pillar of our portal implementation from the outset. Prior to the portal, traceback was conducted via back-and-forth email. When distribution lists are employed, everybody sees everything. Providers are reluctant to share information in this environment. Our Portal changed that, with information being exchanged privately, individually and securely with each provider in

[16] Advanced Methods to Target and Eliminate Unlawful Robocalls, FCC 20-187, CG 17-59, footnote 52

a traceback sequence. This brought hundreds of additional providers into the traceback process, even before participation was mandated by regulation.

Our 2013 proposal detailed a database that underpins a web-based traceback portal; this was how our original implementation was built and it persists today. The transition to a new registered consortium should be seamless to providers and other stakeholders. We propose to import the current (USTelecom) database into our system as of an agreed-to cutover date.[17] We will also incorporate the email templates currently used by USTelecom into our system. This means that traceback from the provider perspective will be virtually unchanged, resulting in little or no disruption to the current process. We also commit at this time that if, at any point in the future, ZipDX is replaced as the registered consortium, we will similarly work cooperatively with our successor as directed and permitted by the Commission to effect a seamless transition.

Traceback sourcing, ZipDX has engaged with enforcement authorities and providers on this matter and helped develop the guidance and the format for submission of traceback candidates. Perhaps most significantly, ZipDX has worked with analytics providers, and in particular YouMail, to initiate and refine and streamline the routine sourcing of tracebacks of unlawful robocalls received by a wide swath of American consumers. Traceback candidates are prioritized by the scope of the campaign and the severity of the violation(s). We have demonstrated that this is a highly effective way of finding persistent facilitators of unlawful calls. Complementing this data with specific examples from other stakeholders lets enforcers build solid cases.

Near the beginning of the pandemic in 2020, ZipDX was quick to engage with YouMail on COVID-19-related calls and allowed us to generate timely tracebacks. We have also been involved with denial-of-service attacks on public agencies and similar disruptive campaigns where speed was critical.

Working with Enforcement. Giving enforcers what they need to be effective is a key role for the registered consortium. ZipDX has developed an array of automated reports to serve these needs. We have directly supported most of the recent robocall enforcement actions, not just with these reports, but in subpoena responses, with records analysis and affidavits. ZipDX also has made webinar presentations to various enforcement groups. In an effort to assist a group of Attorneys General, we have developed a set of robocall-specific analytical

[17] Advance administrative access to the current system, along with an early database snapshot, will allow us to test the cutover process to avoid any disruption. If we cannot obtain the access to the current database, we can move forward with the provider list and contact information in the FCC's Robocall Mitigation Database.

tools addressing their needs and have a roster of about a dozen that have requested and been granted access.

Our philosophy is that ideally, providers would take action to address unlawful robocall traffic transiting their networks WITHOUT engagement by enforcement. ZipDX has developed tools to automatically alert providers when indications are that such traffic has reached significant levels. When we were active in the operation of the traceback function, we engaged routinely with many providers and saw them implement successful mitigation techniques. The ones that failed to do so are the ones that ended up with the enforcement actions noted above.

Do Not Originate. USTelecom's Policies and Procedures include support for a DNO list, which allows a provider to designate telephone numbers they manage which should never originate calls. Other providers voluntarily reject calls purporting to come from a number on the list.

DNO is not mandated by the TRACED Act or the Commission. As Registrant, ZipDX will continue to support it per the Policies and Procedures, and anticipates streamlining the process for both updating the list and accessing it for call processing.

The Critical Need for Evolving Traceback

As the merits of traceback have been proven in the real word, it has become more integral to the overall fight against unlawful robocalls. Yet the calls continue, providing glaring evidence that the battle has not yet been won.

ZipDX believes that we are now at an inflection point where a next-level push will finally deliver a precipitous drop in this traffic. It requires stitching together the various mitigation elements to which so many have contributed. That includes empowering enforcers to better leverage traceback with new tools and reports.

As noted earlier, the Commission has an expectation that the traceback process will evolve; that drives the need for a nimble and dynamic traceback process. Our history demonstrates exactly that and buttresses our claims of an innovative future. Just as there was an initial incentive for robocallers to learn how to harness the providers networks for their illegal activities, that same incentive will push them to find ways to "beat" the existing traceback process. It is imperative that the Registrant be willing to evolve and stay ahead of the robocallers; it simply will not work to run the existing traceback program on auto-pilot.

During the period that the ZipDX portal was the platform for industry tracebacks, we made it a point to continuously improve. Feature enhancements during our tenure included:

- Support for toll-free tracebacks, obviating the need for a distinct, manual effort.
- Integration of the 499A database into the provider onboarding process.
- Detection of forwarded calls, allowing providers to enter redirecting number data that enabled the traceback to continue without administrative intervention.
- Alerting providers to a call that visited their network more than once, making sure that traceback responses took this into account.
- On-going introduction of new reports, using data to reveal insights.
- A framework for objectively evaluating relative provider performance (we called it a "strike score") and for automatically notifying offending providers to ensure their awareness and encourage timely attention.
- Automating the intake of detailed call examples, such that calls placed in the morning could often be traced back to their source or point of entry by afternoon.

Going forward, we anticipate myriad enhancements, driven by input from stakeholders and prioritization in accord with the relevant committees:

- STIR/SHAKEN will allow bypassing some steps in the traceback process; capturing and parsing IDENTITY headers allows us to quickly take advantage.
- Compliance with the emerging Robocall Mitigation Database (RMD), explained in the Second Report and Order (17-97) referenced earlier, gives providers guideposts to follow when accepting calls. ("[A]ny provider not listed in the Robocall Mitigation Database is out of compliance with our rules"[18]). By cross-checking against the RMD, we can alert providers and their downstream providers to potential out-of-compliance situations. ZipDX is already monitoring the RMD on a daily basis and capturing a change log. This also allows us to proactively notify other providers should the Enforcement Bureau de-list a particular provider.
- With proper legal process, enforcement authorities can get automated reporting and even real-time access to certain traceback information via modifications to our existing per-user access-control-list security.
- Properly authorized enforcement authorities will be able to automatically submit traceback requests and subpoenas.
- An API will allow providers to, at their option, automatically respond to traceback inquiries without human intervention
- The DNO process will be streamlined, allowing authorized providers to submit list updates, and making those updates rapidly available to technology suppliers like TransNexus, that enable providers to implement DNO screening without costly forklift upgrades.

[18] Second Report and Order, 17-97, footnote 340.

- Call Detail Record (CDR) analysis not just for enforcers but providers as well, so that they can gain insights into their traffic before it mushrooms out of control.
- As with the RMD, we already monitor two FTC databases. Our system timestamps adds and deletes to the list of 250+ million numbers in the Do-Not-Call (DNC) database, so we can know with certainty that a number was on the list when a robocaller dialed it. And we capture DNC complaints, so that calling numbers in CDRs can be screened against those appearing in the complaint database.

This is an abbreviated list of examples. We agree with the Commission that the process must evolve. We cannot say with certainty exactly what course it will take, but our zeal to learn and to collaborate with others are key elements of our culture. ZipDX is nothing if not nimble and dynamic.

ZipDX is the Most Qualified Candidate for the Registered Consortium Role

The small but focused ZipDX team brings, in combination, over 100 years of experience developing and deploying technology, with stakeholder delight our top priority, built on a foundation of the highest technical and operational integrity.

Our in-house staff are focused on day-to-day operations. There is sufficient skills overlap and cross-training such that service continuity is maintained even if one team member is unavailable for an extended period.

When we lack expertise in-house, we are quick to collaborate and brainstorm and are always anxious to pursue the best solution regardless of the source. For example, pursuing the Robocall Alliance mentioned earlier, we engaged expert counsel specializing in telecom law and in related structural issues. We regularly tap a broad network of resources.

We have operated the ZipDX telemeeting platform for 14 years, with some current customers on our roster almost since our inception. Our traceback efforts benefit from the same creativity and discipline that has gone into that solution. For the telemeeting service, we buy commodity telecommunications services from various voice service providers. This is via arms-length agreements at market prices and does not impact our neutrality.

Our CEO is the first inventor on ten issued patents related to telecommunications and he is an acknowledged contributor to STIR RFC7340, going back to the inception of that technology in 2014.

ZipDX is a RespOrg and a member of SOMOS' Toll-Free Traffic Pumping group. We are a member of, and contributor to, the Communications Fraud Control Association. We have

presented at industry meetings sponsored by M3AAWG, Hiya, PACE, USTelecom, and others. And we have testified before the Senate Special Committee on Aging.

From inception ZipDX has focused on high availability, with geographically-dispersed locations, real-time database replication, continuous system monitoring and alarming and automatic failover. We have specific instances of our platform for development and testing, and can upgrade our production systems without impacting service. We have feature and bug tracking systems and a support ticketing system, ensuring a disciplined development environment and timely responses to stakeholder requests.

ZipDX Compliance and Certifications

Per the TRACED Act, the Report and Order and Further Notice of Proposed Rulemaking (FCC 20-34, March 27, 2020), and the Enforcement Bureau Public Notice (DA 21-474, April 26, 2021), ZipDX LLC certifies as follows:

1) ZipDX is a neutral third party and will carry out its mandate as the registered consortium in a non-discriminatory manner. ZipDX is a single-member LLC, owned and managed by its founder and CEO, David Frankel. ZipDX has no relationships with third parties, financial or otherwise, that could give a party opportunity to interfere with this neutrality.

2) ZipDX has demonstrated competence in the execution of traceback, both technically and administratively. We have a track record of continuous improvement, including responsiveness to all stakeholders in the traceback process.

3) To avoid any disruption to the established traceback process, we adopt as our initial best practices the Policies and Procedures of the incumbent Registrant. These are included in this document as Attachment A. These practices have worked well. We believe it is most efficient to build on what is working, while adapting as the robocalling landscape evolves.

4) ZipDX will focus on fraudulent, abusive or unlawful traffic. This is explicit in the practices shown in Attachment A. ZipDX's history with traceback has always maintained this focus.

5) With this notice, ZipDX makes explicit our intent to conduct traceback efforts of suspected unlawful robocalls in advance of our registration as the single Consortium.

6) Once selected, ZipDX will remain in compliance with the statutory requirements; conduct an annual review to ensure our compliance with the statutory requirements; and promptly notify the Commission of any changes that reasonably bear on our certification.

We are thankful for the opportunity to apply for this role. We look forward to addressing any questions you (or others) may have, and to refining our plans based on input from you and all other stakeholders.

Respectfully Submitted,

David Frankel
CEO, ZipDX LLC

ATTACHMENT A

BEST PRACTICES / POLICIES & PROCEDURES

Downloaded from
https://www.ustelecom.org/wp-content/uploads/2021/01/ITG_Policies-and-Procedures_2021.pdf

INDUSTRY
TRACEBACK
GROUP

POLICIES AND PROCEDURES

JANUARY 2021

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.[1]

TABLE OF CONTENTS

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.[2]

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.[3]

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;[4] 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 may terminate ITG Steering Committee Membership at any time, in conjunction with the advice of the Executive Committee. In particular, the ITG will terminate ITG Steering Committee Membership for Voice Service Providers that do not continue to adhere to these Policies.

ITG Affiliate Members

ITG Affiliate Members are members of the ITG that 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. To be considered an ITG Affiliate Member, however, the 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 may terminate ITG Affiliate Membership in the ITG at any time, in conjunction with the advice of the Executive Committee. In particular, the ITG may terminate ITG Affiliate Membership for Providers that do not continue to adhere to these Policies and Procedures and/or are identified as the originating Voice Service Provider or U.S. POE for Tracebacks after becoming an Affiliate Member.

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.

ARTICLE 3: TRACEBACK PROCESS

Traceback Initiation and Tracking

The ITG 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 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 public, private, or 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 telecommunications services and other Voice Service Providers from fraudulent, abusive, or unlawful use of, or subscription to, such services. All appropriate information regarding a Traceback shall be made available to the organization that requested the Traceback investigation. 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. In no event shall the information provided by the ITG be used for competitive purposes, such as to gain a competitive advantage.

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.

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) (See Appendix D). 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 for Traceback, the ITG is guided by established principles that introduce reasonable due diligence, integrity and transparency into the Traceback process. The principles dictate that Traceback candidates will only be utilized 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, or the request is made with the approval of the subscriber; 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 validated by the ITG generally through 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 harm from 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, 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 requesting full Incident Data, the ITG will fully comply with those requests.

Subpoenas

In general, the ITG will not share detailed call records and data with law enforcement without an appropriate subpoena, Civil Investigative Demand, or other formal request, except with the consent of the customer that received the illegal call that the ITG traced back. The ITG will fully comply with any lawful request.

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 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 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 that 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.[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 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 Suspicious 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 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) those Voice Service Providers contacted as part of the Traceback investigation, 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 resist providing the requested information. 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 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 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 the ITG without authorization.

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 qualify to be considered for DNO treatment, a number: (1) must be inbound-only; (2) generally 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 generally 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 circumstance 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 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.

APPENDIX C: 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.

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 A list of ITG supporting partners that support the ITG is available at https://www.ustelecom.org/itg-partners.

4 *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.

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.