Industry Robocall Strike Force Report

April 28, 2017

1. Introduction *(AT&T)*

1.1. Overview

On October 26, 2016, the Industry Robocall Strike Force issued a report describing progress made during the first sixty days and outlining a process for continuing the work necessary to develop an industry solution to the robocall problem. The industry committed to continue to work together and to issue another status report in six months. ACT, ATIS, CTIA and USTelecom, who count among their members many Strike Force members, agreed to facilitate that process and work together toward long term goals.

Many industry leaders in robocall mitigation have concluded that there is no "silver bullet" to solve the problem. However, to mitigate the problem of illegal robocalls, the industry is implementing a diverse multitude of evolving mitigation tools and efforts so that it becomes too costly for illegal robocalling campaigns to overcome the industry's dynamic mitigation techniques.

The organizations focused on continuing work in the same areas identified by the Industry Strike Force during the first sixty days:

- Authentication
- Empowering Consumer Choice
- Detection, Assessment, Traceback and Mitigation
- Regulatory Support

Each organization met with their members on a regular basis and the organizations held planning meetings at least twice a month. Additionally, monthly meetings were held with all strike force members.

Over the past six months much additional progress has been made and is outlined in this report. Additionally, this report will summarize how the industry will continue its efforts.

1.2. Description of Organizations and Membership

1.2.1. ACT | The App association ("ACT") represents more than 5,000 app makers and connected device companies in the mobile economy. Organization members leverage the connectivity of smart devices to create innovative solutions that make our lives better. ACT is the leading industry resource on market strategy, regulated industries, privacy and security.

1.2.2. ATIS is a technology and solutions development organization that brings together global ICT companies to advance the industry's pressing business priorities. In addition to the extensive work being done by ATIS and its members to address caller ID spoofing and robocalling, ATIS' nearly 200 member companies are also working to address 5G, Cybersecurity, Smart Cities, the evolution to content optimized networks (eCON), the Connected Car, NFV, unmanned aerial vehicles, emergency services, M2M, quality of service, billing and operations, and more. These priorities follow a fast-track lifecycle of development - from design and innovation through standards, specifications, requirements, business use cases, software tool kits, open source solutions, and interoperability testing.

ATIS also is a founding partner and the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), the global collaborative which has developed the Long Term Evolution (LTE) and LTE- Advanced wireless specifications. It is also a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL).

ATIS' membership is diverse and includes participants from key service providers and vendors, including the following 21 of the 33 Strike Force members: AT&T, Bandwidth.com, Blackberry, CenturyLink, Charter, Comcast, Cox, Ericsson, FairPoint, GENBAND, Google, Inteliquent, LG, Nokia, Qualcomm, Samsung, Sprint, T-Mobile, US Cellular, Verizon, and West.

1.2.3. CTIA represents the U.S. wireless communications industry. With members from wireless carriers and their suppliers to providers and manufacturers of wireless data services and products, the association brings together a dynamic group of companies that enable consumers to lead a 21st century connected life. CTIA members benefit from its vigorous advocacy at all levels of government for policies that foster the continued innovation, investment and economic impact of America's competitive and world-leading mobile ecosystem. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

CTIA created a Robocall Working Group (RWG) in early November 2016, shortly after the October 26th release of the Initial Strike Force Report. Since November of last year, CTIA has engaged in weekly meetings of the RWG, and has facilitated members' substantial progress on making robocall control mechanisms and techniques available to consumers.

Of the 33 Strike Force participants, 15 are CTIA members who participate actively in CTIA's RWG. Participating members are: Apple, AT&T, Bandwidth, Ericsson, Inteliquent, LG, Nokia, Qualcomm, Samsung, Sprint, Syniverse, T-Mobile, US

Cellular, Verizon, West. These members span the wireless ecosystem and include carriers, VoIP providers, handset and equipment vendors, infrastructure suppliers and system aggregators.

1.2.4. USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks. USTelecom's members are comprised of companies of all sizes – urban and rural, publicly traded, privately held, and cooperatives. Collectively, these companies have a distinguished history of serving America's communications' needs.

USTelecom members have long demonstrated their commitment to finding solutions to mitigate robocalls. USTelecom's member companies understand and appreciate the annoyance and potential monetary harms inflicted on consumers and businesses resulting from illegal robocalls. USTelecom has a long track record of working with consumer, industry and regulatory stakeholders on ways to mitigate such harms, and has developed strong relationships with law enforcement agencies at the local, state and federal level. The association has also established an industry working group of more than 20 companies that are committed to working together to fight the robocall problem.

2. Authentication and Other Technical and Operational Work *(ATIS)*

The October 26, 2016, Robocall Strike Force Report (Initial Strike Force Report) noted the significant work that ATIS and its members have done to address issues associated with robocalling and caller ID spoofing. In addition to recognizing the significant progress made as of October 2016, the report also acknowledged the work that ATIS had underway to further resolve technical and operational impacts. This report provides a progress update on these efforts, including a summary of the significant work completed since October and the on-going efforts to craft technically feasible and broadly implementable mitigation tools. As ATIS has noted in its monthly updates to the Strike Force, work to address robocalling and caller ID spoofing began long before the Strike Force was assembled; this work will not stop when the Strike Force ends. However, because of the focus of the strike force and the commitment from the strike force members, ATIS has been able to accelerate its timeline.

2.1. Introduction and Background

ATIS is examining issues associated with robocalling and caller ID spoofing from a number of different perspectives:

- *Technical work*. On the technical front, one of the main focuses of ATIS' work has been the development of the SHAKEN framework and associated governance structure by the ATIS and SIP Forum Joint Network-to-Network Interoperability

Task Force (Joint IP-NNI Task Force). However, ATIS' technical work also includes projects undertaken by ATIS' Packet Technologies and Systems Committee (PTSC) and the Joint IP-NNI Task Force to examine SHAKEN-related Best Practices, Attestation and Origination Identifiers and to develop a framework for the display of verified caller ID; as well as PTSC efforts to: (1) examine the feasibility of using Vertical Service Codes to identify unwanted robocalls; and (2) further analyze its initial recommendations for Integrated Services User Part (ISUP) screening indicator interworking.

- *Testing*. The ATIS Testbed Focus Group has also worked on technical issues associated with the testing of SHAKEN, including the development of SHAKEN test plans. ATIS has also partnered with Neustar Trust Labs to offer the ATIS Robocalling Testbed, a virtualized testbed to advance industry efforts to mitigate unwanted robocalls and caller ID spoofing.
- *Operational Work*. ATIS' Next Generation Interconnection Interoperability Forum (NGIIF) is examining SHAKEN and the proposed governance authority framework to provide operational guidance to facilitate implementation by the industry.
- *Numbering-related impacts*. ATIS' Industry Numbering Committee (INC) is examining potential impacts from the implementation of SHAKEN, the SHAKEN governance framework, and the potential use of vertical service codes to report unwanted robocalls.

Finally, ATIS notes that it has continued to collaborate with other key stakeholder organizations, including CTIA, USTelecom and ACT to share progress and foster cooperation.

2.2. SHAKEN Framework

ATIS continues to make progress on technical issues and operational issues associated with the Signature-based Handling of Asserted information using toKENs (SHAKEN). This work includes publication of the SHAKEN framework, as well work to facilitate industry implementation of this framework.

2.2.1. SHAKEN Framework Publication

As noted in the in the Initial Strike Force Report, ATIS and the SIP Forum accelerated their development of the SHAKEN framework.[1]

ATIS and the SIP Forum successfully completed the efforts on this framework, concluding with its availability in December 2016 and formal publication in January 2017.[2] The SHAKEN framework provides a mechanism for managing the deployment of Secure Telephone Identity (STI) technologies with the purpose of providing

[1] Strike Force Initial Report, Section 1.10.1.
[2] A pre-publication draft was made available in December 2016; final industry approval and publication occurred on January 6, 2017.

cryptographic authentication and verification of telephone numbers associated with calls traversing Internet Protocol (IP)- voice networks. This specification defines the framework for telephone service providers to create signatures in Session Initiation Protocol (SIP) and validate those signatures at the call termination. It defines the various classes of signers and how the verification of a signature can be used toward the identification of illegitimate uses of telephone numbers.

The document has broad industry support, having been approved by both ATIS and SIP Forum under their respective transparent, consensus-based approval processes. Initial feedback has been positive. This document is available to the industry electronically at no charge.[3]

2.2.2. SHAKEN Operational Guidance

A related ATIS work program not referenced in the Initial Strike Force Report was the development and publication of a document providing operational guidance for interoperability when implementing the SHAKEN framework.

ATIS NGIIF developed *Interoperability Standards between Next Generation Networks (NGN) for Signature-Based Handling of Asserted Information Using Tokens (SHAKEN)* as a companion to the SHAKEN framework. It provides Next Generation Network (NGN) telephone service providers with a framework and guidance for interoperability as calls process through their networks implementing SHAKEN technologies ensuring the mitigation of illegitimate spoofing of telephone numbers. This document was published in January 2017. This document is available to the industry electronically at no charge.[4]

2.3. SHAKEN Authentication/Verification/Attestation Best Practices and Additional STIR Use Cases

In the Initial Strike Force Report, it was noted that ATIS was working on the creation of SHAKEN-related Best Practices that carriers would maintain.[5] Work is progressing on these two initiatives within the Joint IP-NNI Task Force.

The first is focused directly on SHAKEN Best Practices. It describes how SHAKEN should be deployed along with guidance on implementing the authentication and verification functions. It shows how SHAKEN components would map onto the network under representative deployment scenarios.

The second initiative is focused on the SHAKEN Attestation and Origination Identifiers, which were discussed in Section 1.5 of the Initial Strike Force Report.[6] This work

[3] This document is available electronically at no charge from the ATIS Document Center at https://www.atis.org/docstore/product.aspx?id=28297 and from the SIP Forum at https://www.fcc.gov/news-events/events/2016/10/second-meeting-industry-led-robocall-strike-force.
[4] This document is available electronically at no charge from the ATIS Document Center at: https://www.atis.org/docstore/product.aspx?id=28298.
[5] Initial Strike Force Report, Section 10.1.7

focuses on how the service provider decides what level of attestation is appropriate, as well as provides guidance on how the Orig ID can be used to help with traceback. This document describes problems associated with originating party spoofing in IP communication networks, identifies potential options and/or Best Practices related to attestation and the use of the origination identifiers, and analyzes the pros and cons of mitigation options.

While work has progressed, there remains a good deal of work to be completed. ATIS and the industry remain committed to completing this work and hope to complete this by end of 2017.

2.4. Joint Lab Prototype Testing

As noted in the Initial Strike Force Report, ATIS had agreed to further progress its work to facilitate prototype testing of SHAKEN.[7] Since the publication of the initial report, ATIS launched a virtualized testbed to advance industry efforts to mitigate illegal robocalls and caller ID spoofing.

The ATIS Robocalling Testbed, hosted by the Neustar Trust Lab, allows the testing of SHAKEN by generating end-to-end calls that include all network functions. The testbed allows service providers and vendors to test their implementations of SHAKEN in a test environment to ensure full interoperability. The testbed can provide various configurations to test individual SHAKEN components or complete network implementations.

The test plans were developed by the ATIS Testbed Focus Group in parallel with the development of the SHAKEN framework. This work started well before the Strike Force, and will continue as the best practices documents identify additional areas for testing. Updates to the test plans to cover extensions to SHAKEN are being considered by the ATIS Testbed Focus Group.

Testing of SHAKEN via the ATIS Robocalling Testbed will be provided at no cost to the industry through the end of 2017. Membership in ATIS is not required -- any service provider with an assigned Operating Company Number (OCN) is eligible to participate. Other parties, such as equipment manufacturers, may participate if they have solutions relevant to the SHAKEN framework available to test.

There has been active outreach to organizations that have previously expressed interest in SHAKEN testing. ATIS notes that active testing is underway. To date, approximately 10 companies have executed or are in the process of executing the relevant agreements to test, and a total of 16 companies have executed the testing NDA that would allow possible future participation in testing.

---

[6] Section 1.5 of the Initial Strike Force Report addresses this issue but does not identify a specific long-term objective associated with this action. Nonetheless, the industry has been working on a related deliverable.
[7] Initial Strike Force Report, Section 1.0.4.

Strike Force members and others interested in learning more about the ATIS Robocalling Testbed may visit https://www.neustar.biz/atis-testbed/index.php.

2.5. Governance Model and Certificate Management Policy Framework

In addition to the development of the underlying technical framework (i.e., SHAKEN), there is work underway to advance the governance model associated with this framework. The three initiatives below would define the ecosystem in which end-to-end cryptographic authentication and verification of the telephone identity would occur.

2.5.1. Governance Model/Framework

One of the long term goals identified in the Initial Strike Force Report was to further progress the SHAKEN governance model.[8] Significant progress has been made on this deliverable by the Joint IP-NNI Task Force.

The SHAKEN governance model identifies the key roles / functions involved in distributing and managing SHAKEN certificates. The model envisions a governance authority that would oversee a policy administrator, which would determine who is entitled to get SHAKEN certificates, which would be issued by certificate authorities.[9] The chart below provides a high-level view of the various roles, including what is currently addressed by the governance model ("in scope") and what is being defined through other work ("out of scope" for the framework but addressed in section E.3 below).

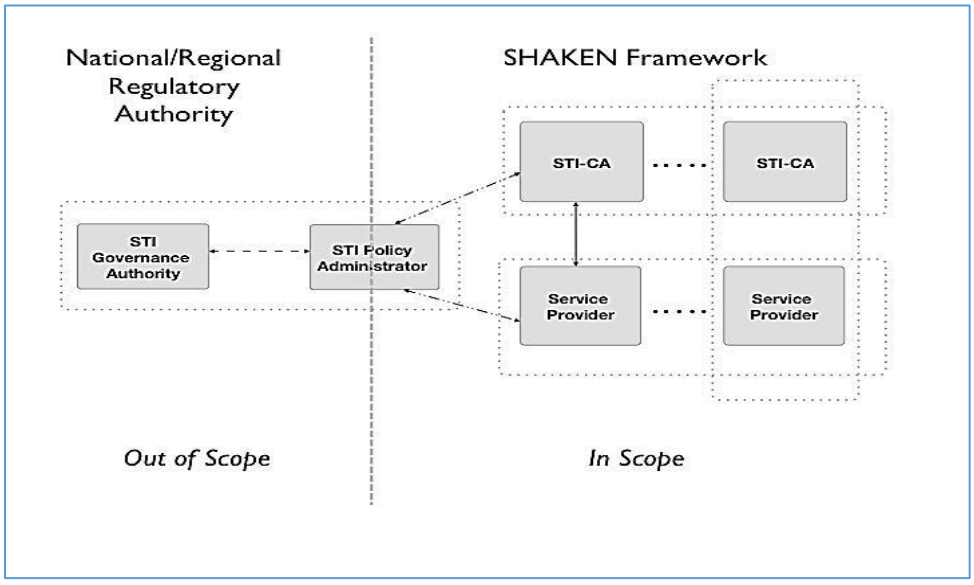


Chart 1 -- SHAKEN Governance Model

[8] Initial Strike Force Report, Section 1.10.7.

[9] The Initial Strike Force Report identified the role of the TA Administrator, which would do the manual process of working with service providers to validate they are who they say they are and manage credentials of Telephone Authorities to have a secret key and the Service Providers to do Certificate Signing Requests (CSR) transactions with the Telephone Authorities. This role is now defined under the draft framework as the STI Policy Administrator.

The model would specify the protocols that will be used to obtain certificates and the "key" that service providers will obtain from the STI Policy Administrator to prove that they are entitled to get SHAKEN certificates. ATIS notes that, while this model identifies at a high-level the functions associated with the STI Governance Authority and policy administrator, it does not specify the structure of, or detailed functions associated with, the STI Governance Authority or STI Policy Administrator.

The work to ensure that the proposed model results in an implementable solution that is both technically and operationally feasible has been complex. Proposals to align with existing service provider certificate management processes are expected to facilitate and expedite implementation. This work is expected to be completed in 2Q2017.

2.5.2. Framework Operational Guidance

ATIS NGIIF is developing a document examining the operational implications of the SHAKEN governance model and certificate management. This document will complement the governance framework currently under development by the Joint IP-NNI Task Force (see section E.1 above). The target is to align the publication date with Joint IP-NNI Task Force governance document.

2.5.3. Governance Ecosystem

ATIS is also working with its members to identify the detailed functions associated with the governance framework. This work will complement the governance framework document by examining the ecosystem that will be necessary to implement that framework by defining in a more granular fashion the roles of the STI Governance Authority and STI Policy Administrator. This work, which is expected to result in consensus-based proposal for the structure of the ecosystem that would be necessary to support the implementation of SHAKEN by the industry, is expected to be completed in 2Q2017.

2.6. Display Framework

The Initial Strike Force Report noted the work that ATIS had underway to further progress its Signaling Verification and Analytics Information, and Display Framework.[10] The industry continues to make progress on the draft *Framework for the Display of Verified Caller ID*. Additionally, ATIS notes that there are other initiatives within the Joint IP-NNI Task Force to: (1) assess mechanisms to signal verification to legacy call display; and (2) provide input to 3GPP and track progress on "verstat" TEL URI parameter to signal verification to SIP client. All three deliverables are anticipated to be completed by the end of 2017.

[10] Initial Strike Force Report, Section 1.8.

2.7. Feasibility of Using Vertical Service Codes to Report Unwanted Robocalls

The Initial Strike Force Report recommended that ATIS investigate the feasibility of using vertical service codes (i.e., *XX codes) to report unwanted robocalls.[11] Two initiatives are under development on this topic.

The first initiative is being undertaken by ATIS PTSC. Its objective is to examine the feasibility of using these codes to report unwanted robocalls, including whether codes in use for other services (such as *57- Call Trace) could be used, the benefits and challenges of sharing codes and/or selecting a new code and effective alternatives to the use of vertical service codes. The PTSC (and subsequently Joint IP-NNI Task Force) reviewed contributions on the use of VSC and agreed with the preference to use alternative methods to report robocalls, such as using web portals and smartphone apps, rather than using VSC.

ATIS INC has also examined this issue and will address any numbering related impacts, including the development of and/or revision of industry guidelines should the use of an existing or new vertical service code be recommended. INC's initial review of the existing framework draft identified no unusual numbering-related impacts from the use of these codes.

2.8. Technical Review on SS7 Feasibility

As noted in the Initial Strike Force Report, ATIS' *Technical Report on Use of the ISUP Screening Indicator for Conveying Caller ID Authentication Information* was completed in October 2016.[12] This Technical Report assessed three potential industry solutions for using the ISUP Screening Indicator to convey Caller ID Authentication information. The industry Strike Force evaluated these potential solutions and identified one of the proposed solutions[13] as the most viable, in that it would provide the greatest integrity of the Calling Party Number (CgPN), while being the least impactful to existing customer expectations with respect to delivery of CgPN.

Based upon the completed work and the input from the Strike Force, ATIS PTSC has initiated a project to further analyze one of its recommendations for ISUP screening indicator interworking. This work has been targeted for completion by the end of 2017.

---

[11] Initial Strike Force Report, Section 2.5.2. Although VSCs are originally defined for TDM networks, concepts could be extended to SIP networks for SHAKEN

[12] Initial Strike Force Report, Section 1.10.3. This ATIS technical report is available from the ATIS Document Center: at: https://www.atis.org/docstore/product.aspx?id=28295.

[13] This solution involves the successfully verified signed PAI or FROM headers, attesting that the device can use the TN, being interworked into the CgPN with a SI value of "user provided, verified and passed," but differs from other solutions in that, if the PAI or FROM headers are not signed, a "network provided" number (e.g., pseudo number that is unique to each carrier) is populated into the outgoing ISUP CgPN parameter with an indication of "network provided" in the SI field.

2.9. Other ATIS Strike Force Work

In addition to the work projects described above, ATIS has also worked cooperatively with the other stakeholder organizations on Strike Force matters. ATIS has provided feedback, for example, to the USTelecom Industry Traceback Group (ITB Group) on Canadian service provider interest in the group, resulting in a new service provider participant.

ATIS has provided feedback from ATIS INC to this group noting that 555 numbers may be good candidates for Do Not Originate trials. These numbers should not be used for any natively legitimate purpose to originate calls, and thus any originating use would identify the call as spoofed.

2.10. Conclusion

ATIS notes that the efforts to mitigate robocalling and caller ID spoofing are complex, with a significant number of interdependencies. However, ATIS and its members are committed to addressing these issues with the requisite urgency, including relevant work outside of those projects identified in the Initial Strike Force Report. ATIS' work is a careful balance of the need for quick action with the need to develop implementable, technically- and operationally-effective and sound mitigation techniques that reflect the consensus of the industry.

3. Empowering Consumer Choice

Consumer choice is critical to effectively managing illegal robocalls. Many marketing, charitable and other communications are wanted and lawful, while unscrupulous telemarketers abuse technology and flout the law. Consumers should be empowered to better control their communications. Fortunately, mitigation tools are available in the form of applications that are providing increased options to consumers. And industry associations are acting as force multipliers for company efforts and consumer education.

3.1. App Development *(ACT)*

As the world has quickly embraced mobile technology, the hyper-competitive app ecosystem continues to produce more innovative and more efficient solutions that leverage mobile technologies to drive the global digital economy across modalities and segments, augmenting consumer interactions and experiences throughout their personal and work lives.

Service providers, manufacturers, app developers, government, and consumers all have a role in reducing unwanted robocalls. ACT agrees that third-party apps can play a critical role in empowering consumers to control robocalls. As a part of our commitment to stop unwanted robocalls, ACT, representing the developer community, has worked within the

Strike Force to support the development of more effective apps to increase consumer control over robocalls. ACT has completed three key deliverables following the completion of the Strike Force. They are:

- A public-facing website that provides technical information and recommendations for current and potential robocall control app developers, including technical updates related to changes to information provided by networks and vendors on call spoofing or signaling systems that applications can harness. The website provides app developers information on privacy and privacy policy best practices. ACT designed this information to make it easy for app developers to capitalize on the approaches developed by the Strike Force and to create innovative new solutions.[14]
- Targeted outreach to the ACT's members, including more than 5,000 app companies and IT firms from across the mobile economy to educate members about opportunities to develop robocall control apps.
- An online workshop for developers offering both real-time participation and access to ACT's archives. The workshop will work to catalyze the creation of new apps by helping developers quickly get up to speed on the technical and policy considerations behind robocall control apps.[15]

ACT is pleased to satisfy its obligations as part of the Strike Force, and we are proud of the incredible work every member has contributed in taking meaningful steps to contribute to the mitigation of unwanted robocalls.

While further innovative apps are in development, apps today are already playing a major role in mitigating unwanted robocalls (examples include AT&T Call Protect, Nomorobo, Hiya, PrivacyStar, and many others), and will continue to do so. We encourage developers, consumers, and other stakeholders to explore the apps available today; and to collaborate and develop innovative apps to mitigate unwanted robocalls.

As discussed in this report, the Robocall Strike Force is examining the development of a standardized framework for delivering information from networks to devices with the aim of better empowering consumers to make informed call handling decisions. Moving forward, ACT will continue to encourage its members to rely on these important consensus documents as they find new and innovative ways to provide for consumers to take control over robocalls.

3.2. Consumer Education Efforts by Strike Force Members

[14] http://actonline.org/2017/03/28/robocalls-app-developers/
[15] *Id.*

3.2.1. Wireless

The wireless sector has been actively working to address abatement of illegal robocalling, and promoting consumer awareness of existing tools.

With release of the Industry Strike Force Report, CTIA convened the RWG and immediately began work on wireless stakeholder engagement, working with other trade associations, and committing to and providing regular updates to the Industry Strike Force. Specifically, since CTIA convened its RWG:

- CTIA has highlighted and facilitated members' efforts to keep their consumer-facing robocall prevention content current in collaboration with Industry Strike Force initiatives.
- CTIA conducted a survey of its members to learn about spam-scoring services available in the marketplace today.
- CTIA convened six third party vendor presentations to educate members on innovative robocall mitigation techniques.
- CTIA has integrated a robocall mitigation use case into its ongoing Automated Cyber-Threat Information Sharing (AIS) Pilot being sponsored by CTIA's Cybersecurity Working Group.
- CTIA is working with members on the best ways to display verified caller ID information graphically on a user's handset.

CTIA' s consumer education efforts have been robust and effective. CTIA's webpage on Robocall Mitigation provides a comprehensive list of well over 80 mitigation apps and step-by-step video instructions for Android, BlackBerry, iOS and Windows devices. Many, if not most, of these apps are free. Carriers often refer their customers to the CTIA website to guide consumers to the rich variety of available third-party apps. Likewise, CTIA and other associations have supported ACT in its efforts. CTIA has updated its website to contain references to numerous tools, including apps, as well as important consumer tips. Go to: http://www.ctia.org/your-wireless-life/consumer-tips/blocking-robocalls.

- In March 2017 alone, CTIA's robocall consumer tip pages received over 15,000 views
- Since November 2016, CTIA's robocall consumer tip pages has received an average of nearly 10,000 views each month

Several carrier and vendor members of CTIA's RWG have their web resources on robocall mitigation mirrored on the dedicated FCC Resource webpage: http://fcc.gov/unwanted-calls. In turn, CTIA uses social media to heighten public awareness on robocall mitigation. CTIA also facilitated members' efforts to keep their consumer-facing content current in collaboration with Industry Strike Force initiatives.

CTIA looks forward to continuing to support the efforts of the Industry Strike Force and other industry efforts. Attention will be directed to authentication, empowering

consumer choice, and efforts to automate what are today the largely manual and iterative Traceback and/or Do Not Originate processes, which are described in detail below.

CTIA considers illegal robocalling to be a potential cyber threat. So, looking ahead to automation, CTIA has integrated a robocall mitigation use case into the ongoing Automated Cyber-Threat Information Sharing (AIS) Pilot sponsored by CTIA's Cybersecurity Working Group. This pilot seeks to build toward automated examination and sharing of call detail records associated with suspected robocalls to inform Traceback and Do Not Originate capabilities.

3.2.2. Wireline

After the initial meeting of the Industry Strike Force at the FCC on August 19, 2016,[16] USTelecom worked with its association members and Strike Force participants to increase consumer awareness on robocall issues. After the conclusion of the first Strike Force meeting, USTelecom and CTIA, in coordination with the FCC, published consumer-centric websites providing them with information on robocall issues, including consumer tools available to them.[17]

USTelecom's webpage includes a broad variety of consumer-centric information regarding robocalls, including consumer safety tips and robocall mitigation tools. The website also includes a link to several tools available to consumers to block and/or mitigate robocalls on a range of consumer voice platforms, including traditional TDM networks, IP networks and wireless services.[18] A link to USTelecom's website is also available through the FCC's robocall portal. Several consumer groups and other organizations also maintain resources on their respective websites educating consumers about robocall issues.[19] In addition, several companies participating in the Industry Strike Force have also taken steps to educate customers about robocalls, as well as make mitigation tools available to consumers on their company websites.[20]

---

[16] *See*, Public Notice, FCC to Host First Meeting of Industry-Led Robocall Strike Force, DA 16-917 (August 12, 2016); see also, FCC website, First Meeting of Industry-Led Robocall Strike Force (available at: https://www.fcc.gov/news-events/events/2016/08/first-meeting-industry-led-robocall-strike-force) (visited March 30, 2017).

[17] *See*, USTelecom website, Robocalls (available at: http://www.ustelecom.org/issues/robocalls) (visited April 22, 2017); *see also*, CTIA website, How to Stop Robocalls (available at: http://www.ctia.org/consumer-tips/robocalls) (visited April 22, 2017).

[18] *See*, USTelecom website, *Robocalls* (available at: http://www.ustelecom.org/issues/robocalls) (visited April 25, 2017).

[19] *See e.g.*, Consumer Reports, *Robocall Blocker Review*, August 14 (2015) (available at: http://www.consumerreports.org/cro/magazine/2015/07/robocall-blocker-review/index.htm) (visited April 25, 2017); *see also*, AARP website, *Robocalls* (available at: http://blog.aarp.org/tag/robocalls/); AARP website, Scam Alert (available at: http://blog.aarp.org/2014/08/01/how-to-avoid-robocall-scams/) (visited April 25, 2017); FTC website, *Consumer Information, Robocalls* (available at: https://www.consumer.ftc.gov/features/feature-0025-robocalls) (visited April 25, 2017).

[20] *See e.g.*, AT&T website, *Call Blocking options: Nomorobo* (available at: https://www.att.com/esupport/article.html#!/u-verse-voice/KM1074689) (visited April 25, 2017); CenturyLink

There is strong industry support for increased consumer education about robocalls, to include increasing awareness of the threat, as well as tools available to consumers. Such an approach can have a tangible and positive impact on robocall issues, and educational outreach has been previously identified by the FCC and the Federal Trade Commission as an essential component to raising awareness of this issue.[21] Public outreach measures have been successfully implemented by the federal government in the past and are ideally suited in the current context. Whether implemented on a broad public relations scale, or through targeted multi-industry efforts, such outreach measures ensure that valuable information is disseminated and shared amongst target audiences.

3.3. Industry Input from Non-Strike force members

3.3.1. Wireless

CTIA has worked to bring non-members into the discussion and activity on illegal robocall abatement. CTIA convened numerous meetings to share technology and solutions. As discussed in the October Strike Force report, CTIA undertook the task of working with members to provide robocall mitigation information to customers.

CTIA surveyed its RWG members and learned about spam-scoring services in the market today. As noted, CTIA then reached out to the third party vendor community, and facilitated presentations from six companies to the RWG regarding robocall mitigation opportunities. The companies below presented:

- Cequint: Provides spam scoring, based on real-time network data analytics to ensure that legitimate enterprise calls to customers are not placed incorrectly on a blacklist. https://www.cequint.com/personal/
- Hiya: Provides network-based caller ID and spam detection and protection natively integrated for all clients, and O/S platform independent. https://hiya.com/#page-top

---

website, *Ways to block unwanted calls from your home phone* (available at: http://www.centurylink.com/home/help/products/calling-features/ways-to-block-unwanted-calls-from-your-home-phone.html) (visited April 25, 2017); Verizon website, *What are robocalls* (available at: https://www.verizon.com/support/consumer/consumer-education/robocalls) (visited April 25, 2017); Frontier website, *Call Block & Priority* (available at: https://frontier.com/helpcenter/categories/phone/calling-features/call-block-priority-residential) (visited April 25, 2017).

[21] *See e.g.*, Public Notice, FCC to Host Consumer Webinar on Dealing with Robocalls (released February 2, 2017); *See e.g.*, Comments of FTC Chairman Jon Leibowitz, FTC Robocall Workshop, October 18, 2012 (noting that the FTC "pride ourselves on the fact that we take a multi-faceted approach to consumer protection issues that includes enforcement, education, policy, and advocacy." (available at: https://www.ftc.gov/sites/default/files/documents/public_events/robocalls-all-rage-ftc-summit/robocallsummittranscript.pdf) (visited April 25, 2017). *See also*, FTC website, *Phone Scams* (available at: https://www.consumer.ftc.gov/articles/0076-phone-scams) (visited April 25, 2017); FCC website, *Unwanted Calls* (available at: https://www.fcc.gov/unwanted-calls) (visited April 25, 2017).

.

- iconectiv: Certified Caller ID: Demonstrated the process of certificate assignment (and revocation) pursuant to STIR/SHAKEN protocol. http://iconectiv.com/thought-leadership/existing-robocalling-and-spoofing-mitigation-techniques
- Neustar: Smart ID product, which integrates APIs on: CNAM (to include business logos); subscriber insights; and certified caller ID. Includes Neustar's Trust Lab, selected by ATIS as its Robocalling Test Bed. https://www.neustar.biz/communications/caller-id
- Nomorobo: A wireless, network-agnostic application based on new API capabilities available with the release of iOS 10 and higher. A nominal subscription-based service, it allows the download of updated number blacklists to the iPhone. http://www.nomorobo.com/
- PrivacyStar, a First Orion company: Originally app-based, expanded their in-network deployments which leverage data analytics and call heuristics to aid in call labeling and categorization and offer consumers more information to reduce blocking of "wanted" robocalls (pharmacy, school, enterprise). https://www.privacystar.com/

CTIA and its members are encouraged by the level of communication about these issues, and look forward to pressing forward on new solutions and approaches, including those developed by third parties. In fact, some CTIA members already make services from these third party vendors available to their customers.

3.3.2. Wireline

Since the start of the industry-led Strike Force efforts, USTelecom has also made significant outreach and inroads to non-Strike Force members. For example, in January, 2017, USTelecom met with representatives from Duke Energy, which is leading a coalition of approximately 90 electric utility organizations called "Utilities United Against Scams" (Utilities Coalition). The Utilities Coalition was formed last year by Duke Energy to address and combat ongoing fraud targeted towards electric utility customers through illegal robocalls. The calls would fraudulently advise consumers that their electricity services would be cut off, unless payment was immediately submitted.

In January, 2017, USTelecom delivered a presentation to the coalition regarding the ITB Group[22] efforts, and USTelecom will also be attending its first face to face meeting in Fort Worth, Texas in May. In addition, USTelecom was able to facilitate discussions between the Utilities Coalition and other industry partners in order to shut down several toll free numbers that were hosting fraudulent interactive voice response (IVR) systems that were spoofing legitimate electric utility companies. Fraudsters were using the spoofed IVR systems to facilitate communications between targeted

[22] See sections below, "USTelecom Efforts on Detection, Assessment, Traceback and Mitigation" and "USTelecom Status of Traceback Initiatives" for further details on the ITB Working Group.

consumers and the scammers (i.e., consumers were led to believe they were contacting legitimate electric utility companies).

As a result of this coordination, the Utilities Coalition was able to identify toll free numbers being used in the IVR scams and have them removed from service. This industry-wide coordination is ongoing, and the group is working to establish a more streamlined and effective system for electric utilities to remove these fraudulent IVR numbers from service on an expedited basis.

In addition to this effort, USTelecom continues its outreach and coordination with various federal agencies regarding areas of potential cooperation. For example, USTelecom staff met with IRS investigators in September, 2016, to discuss the IRS scam, and additional cooperation between industry and the agency. As a result of these efforts, USTelecom staff conducted in-person training for Treasury Department staff, including Treasury Inspector General for Tax Administration (TIGTA) personnel on November 9, 2016. The class, "Telephony 101 and Robocall Fundamentals" provided Treasury Department personnel with an overview of how telecom networks function, the nature of robocalling, the wide variety of robocall schemes and industry traceback efforts.

These efforts are ongoing, and in addition to the IRS, USTelecom has coordinated with Health and Human Services and Immigrations and Customs Enforcement on industry-led efforts to combat robocalls. Finally, USTelecom has also conducted outreach to various industry stakeholders engaged on the robocall issue. For example, USTelecom has met on several occasions with various stakeholders deploying robocall mitigation tools, including several vendors of telecommunications services. USTelecom intends to continue this outreach and coordination in the coming year.

3.4. Network to Device Display

3.4.1. Wireless and other IP-based Networks

The telecommunications industry has been working on the complexities surrounding on-device displays about illegal robocalling. To date, industry efforts on Robocall Mitigation have focused on the transmission of "verified Caller ID" using the "STIR/SHAKEN" framework where a SIP-based network is available, e.g., a VoLTE network supporting wireless subscribers. Using this protocol can enable a carrier to determine if an originating service provider has authenticated a particular telephone number. Industry has been considering how verified Caller ID information can and should be displayed on a user's wireless handset to enable real time decision making by consumers about incoming calls. Questions include whether there should be standardization with respect to a minimum set of display requirements or whether that is best left to the network, OEM and app communities.

Industry participants are investigating how an OEM or carrier can graphically display verified caller ID information on the user's handset. Work on network-to-device

display is in early stages and ongoing. CTIA is working with its carrier, handset and system vendor members, and standards organizations, on how to best display information to the consumer about an incoming call. Considerations include whether minimum set of requirements for network-to-device display is preferred, versus giving carriers greater flexibility to pursue innovation in graphical design from the handset, system vendor, and carrier communities.

3.4.2. Wireline

On the wireline side, substantial innovation is ongoing to address the display challenges associated with existing customer premises equipment. For example, for several months Verizon has been trialing, to millions of its wireline customers, a new service that warns about potential spam by inserting a warning indication in the Caller Name field of the home user' phone display that the incoming call may be spam related. One advantage of this approach is that because it rides on the CNAM database that carriers use to associate a calling party name with a particular telephone number, it uses the customer's existing 15-character display, and it does not require either a VoIP connection or the transmission of a new SS7 field. This trial is an implementation of the patented prototype technology that Verizon presented to strike force members last fall, which Verizon has offered to share with interested carriers.

3.5. Industry Member Activity

Industry participants and Strike Force members continue to improve and expand mitigation tools to combat illegal robocalling. Much of this work cannot be made public because it would provide too much information to the robocallers but here are some examples of what is being done. The market is working.

- AT&T: Launched AT&T Call Protect in December 2016 as a free network service. It allows customers with iPhones and HD Voice-enabled Android handsets to automatically block suspected fraudulent calls. It can flag suspected spam calls so the customer can choose whether to answer or not. And, using the interface provided by the AT&T Call Protect app, customers can manually block an unlimited number of specific telephone numbers for 30-day intervals. The customer can download the app via the AT&T website or on their device through the App Store. Network call data analysis and heuristics that power this solution are provided by Hiya. In addition, AT&T blocked its billionth unwanted robocall in cases where its business contracts allow it to block impermissible traffic using a new program that detects violators through network data analysis.
- Comcast: Comcast offers Nomorobo, a free cloud-based service that hangs up on or blocks illegal robocaller or telemarketing calls from calling the intended home telephone number, to its wireline customers
- Sprint: Sprint offers Premium Caller ID service on a subscription basis. It now includes, for select Android smartphones, the ability to not only the ability to identify a higher percentage of nuisance calls, but also an option to block them. This solution

directly leverages data and network intelligence powered by a partnership with Cequint, a wholly owned subsidiary of Transaction Network Services (TNS).

- T-Mobile: T-Mobile launched Scam ID in March 2017 as a free, network-based automatic service that identifies calls from known phone scammers, across all handset platforms, on smartphones and feature phones. If a scam call is detected, the Caller ID will display "Scam Likely" on the device, giving customers the option to answer, or permanently block the number. Customers that choose to invoke Scam Block, another free service, will have all calls from known scammers blocked. These solutions are powered by network call data analysis and heuristics provided by PrivacyStar, a First Orion company.
- Verizon: Verizon has used the CNAM-based solution described above to warn more than four million wireline Fios Digital Voice customers about calls identified by Verizon's analytics engine and its robocall mitigation team, including calls relating to the well-known IRS impersonation scam. Verizon's network team also worked with Nomorobo to develop a "one click" solution that simplifies Fios Digital Voice customers' ability to sign up for that third-party blocking service. And since November 2016, Verizon Wireless has been trialing a service that scores all incoming calls to its Caller Name ID customers, identifying potential spam and calling-out the level of risk with a "risk meter." The service is powered by Cequint, a wholly owned subsidiary of Transaction Network Services (TNS), and is currently available on ten Android devices. Verizon expects a broader product launch later in 2017.
- Apple: Apple introduced CallKit for iOS 10 and higher. API developers can create a call directory app extension to identify and block incoming callers by their phone number. This opens the iPhone ecosystem to an important call control capability, for devices running iOS 10 and higher, across all service provider networks. https://developer.apple.com/reference/callkit
- West: In response to the rise of spam calls, West is working with the various call blocking solution providers to promote decision support tools for the entities whose numbers have been compromised.
- Google: In late 2016, Google introduced spam protection functionality on the Google Phone application for Pixel, Nexus, and Android One devices, which warns users about potential spam callers and provides users with the choice to block and report these numbers. (*See, e.g.*, https://support.google.com/pixelphone/answer/3459196) The user interface and reporting aspects of Google Phone spam protection have also been made openly available at no cost to third parties via the Android Open Source Project (https://source.android.com/). In addition, there are plans to provide platform APIs in upcoming builds of Android that would offer new forms of spam solution support for carriers and manufacturers.
- Strike Force members worked with the CFCA in developing customer education messaging about how consumer can protect themselves from fraud, including the attached the attached fraud-related message: https://www.youtube.com/watch?v=rE53QDNP8Is.

4. Detection, Assessment, Traceback and Mitigation *(USTelecom)*

In June of 2015, USTelecom formed a Robocall Engineering Working group. USTelecom invited its carrier members to participate in this working group with the goal of easing and simplifying the process of tracing the origins of robocalls, otherwise known as traceback. During the course of these Robocall Engineering Working Group efforts, the group noted that the sharing of certain network intelligence and traceback information among its participants could and did lead to the successful thwarting and mitigation of unwanted and illegal phone traffic. A key lesson learned from USTelecom's extensive experience and leadership in traceback efforts is that with investments in personnel and IT systems, along with providers' contact information for traceback and subpoena requests being readily available, voice providers can establish the systems and processes needed to efficiently process requests (whether government subpoenas or requests from other carriers) to identify the source of suspicious traffic traversing their networks. Unfortunately, while numerous providers have formally joined our traceback efforts, and many others cooperate in good faith in tracebacks, there are still upstream carriers who refuse to cooperate, which prevents carriers from tracing these malicious calling events back to the origin of the call.

In May of 2016, the Robocall Engineering Working group felt it would be beneficial for wide-scale industry participation, and to include service providers from outside of USTelecom's membership in these robocall mitigation efforts. USTelecom therefore developed a framework for participation and governance and began to invite numerous service providers to participate in traceback efforts.

Many service providers accepted the invitation and the terms of the framework. On June 28, 2016, USTelecom conducted the first Industry Traceback Working Group (ITB Group) conference call. There are currently twenty-one members of the ITB Group, which includes traditional wireline phone companies, wholesale carriers, wireless providers, and cable companies. The membership also includes foreign carriers (e.g., Bell Canada), and non-traditional voice providers (e.g., Google). USTelecom will continue to reach out to industry stakeholders in an effort to continue expanding membership in the ITB Group.

The ITB Group conducts biweekly conference calls to discuss malicious calling events that were observed on the members' respective networks. Various network actions and mitigation practices are discussed and shared with the group. Between conference calls, when a malicious calling event occurs on one or more networks, the ITB Group is alerted via emails that are sent out by the detecting service provider. The remaining group members conduct network scans, research and analysis to determine if these events are occurring on their respective networks. Each ITB Group member explains their observations, their respective notification actions, network actions, and shares any traceback information with the rest of the working group.

Subsequent to the October meeting of the Industry Strike Force, USTelecom and the ITB Group focused its efforts on completing a Do Not Originate (DNO)[23] trial in order to assess the feasibility of DNO as a robocall mitigation tool. During November and December of 2016, USTelecom staff and individual ITB Group members reached out to relevant stakeholders to identify potential DNO candidates. This included outreach to industry trade associations, individual companies, and government stakeholders. Once suitable candidates for DNO were identified, a series of trials were conducted during January and February of 2017.

Finally, the ability of carriers to institute a DNO varies by ITB Group members. Each ITB Group member oversees a diverse range of network facilities, some of which are more capable of instituting DNOs in a more seamless manner. In addition, the resources and capabilities available to each of the ITB Group members also varies, with some members having fully staffed fraud and network engineering departments operating on a round-the-clock basis. In addition, implementation of DNOs by individual ITB Group members was wholly voluntary throughout this process.

4.1. USTelecom Status of Traceback Initiatives

With the establishment of the ITB Group, efforts were primarily focused on the mechanics and processes for initiating industry traceback efforts. Initial efforts of the group were focused on identifying possible illegal robocall incidents, and threat intelligence was shared between ITB Group members. This initial information sharing effort enabled ITB Group members to scale the scope of suspected robocall incidents, and enabled individual ITB Group member efforts to institute mitigation measures on their own networks to address these call incidents.

As the ITB Group grew in membership size, these information sharing efforts significantly accelerated awareness of such incidents across a broad range of industry stakeholders. In addition, these initial efforts facilitated coordination between individual ITB Group members, who could more easily cooperate on analyzing suspected robocalling events. Also, efforts have been implemented for faster responses to traceback requests, by working in conjunction with ATIS to update ATIS' Service Provider Contact Directory (SPCD).[24] The SPCD, available upon request across the industry ecosystem (e.g., service providers, regulators and enforcement bureaus) to provide contact information for reporting or passing along trouble reports to interconnecting companies, has been expanded to include contacts related to traceback and for subpoena requests. As more providers submit their contact information for the SPCD, traceback efforts can be investigated in a more expeditious manner.

In late 2016 (between November and December), USTelecom staff began exploring enhancements to its initial efforts. These reforms were instituted to make the ITB

[23] See section below, "USTelecom Status of Do Not Originate Initiatives" for further details on the DNO.
[24] See section below, "Work with enforcement to shorten the cycle time between identification and action to stop illegal activity" for further details on the SPCD.

Group's traceback process more focused and more effective in tracing back specific call paths closer to their point of origin in the network. These reforms included: 1) more targeted traceback requests; 2) expanded outreach to upstream carriers; and 3) detailed cataloguing of information collected during individual tracebacks.

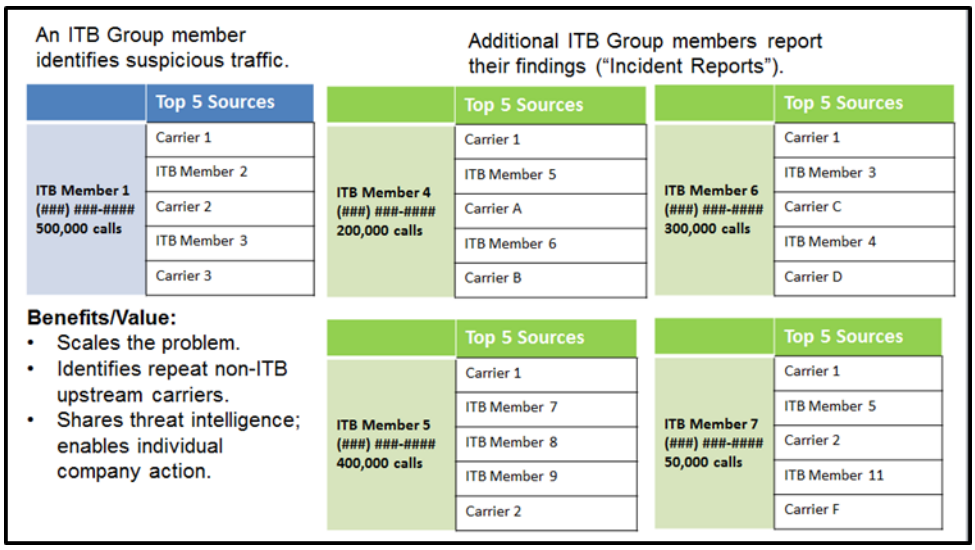
Regarding the first reform, ITB Group members focused on exercising their ability under Section 222(d) of the Communications Act, which allows carriers to share CPNI in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services."[25] The sharing of such information by telecommunications providers can benefit consumers by enabling providers to quickly, efficiently and cooperatively identify the true source of fraudulent, abusive or unlawful calls, including robocalls. In instances where calls are traced to their point of origin, this often enables investigating providers to work with the originating carrier to cease such calls initiated by its customer. Such efforts are also extremely valuable to law enforcement, since carriers' ability to trace calls through several networks can substantially assist law enforcement personnel in subsequent investigations.

Regarding expanded outreach to upstream carriers, USTelecom initiated an effort whereby non-ITB Group upstream carriers were contacted by USTelecom staff. Because any particular call flow can include both ITB Group members, and non-ITB Group members, it was essential to reach out to carriers in the latter category to encourage them to participate in the industry-led effort to identify the source of illegal robocalls.

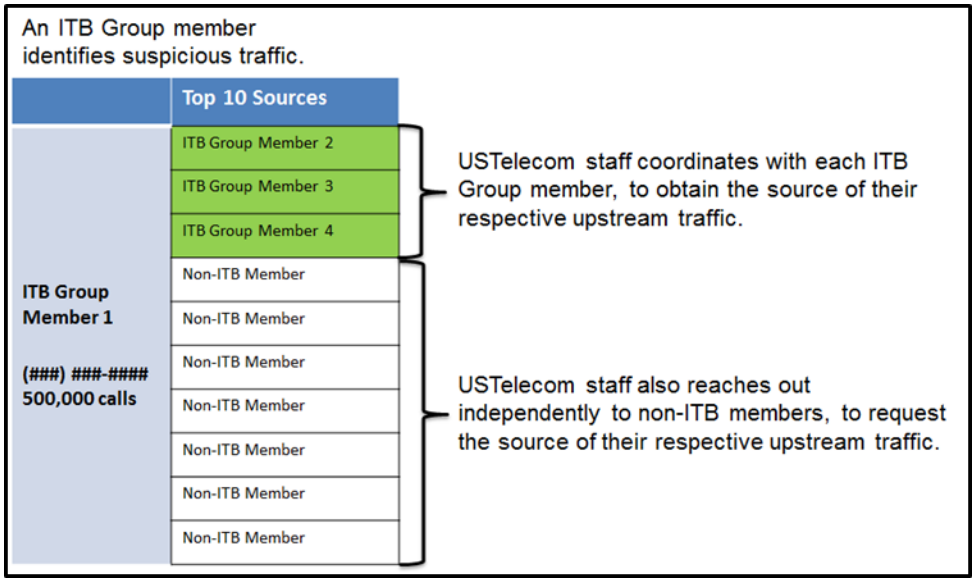
Finally, USTelecom instituted a process whereby the association catalogues certain information relating to traceback efforts by the ITB Group. The information is retained in a password-protected Microsoft Access database by USTelecom. Once a traceback effort is initiated by an ITB Group member, a reference number is assigned for that particular call incident. This information includes the requesting ITB Group member, the date of the calling incident, the date the traceback effort was initiated within the ITB Group, the volume of calls associated with the calling incident, and the phone number associated with the calling incident (Traceback Number).

Once this data is entered, ITB Group members are asked to scan their respective networks for the Traceback Number to see whether it has transited their respective networks. If this is the case, ITB Group members report back to USTelecom with a listing of the top 5 or 10 upstream carriers (that may include both ITB Group members, and non-ITB Group members), as well as associated call volumes (Incident Reports). The Incident Reports from responding ITB Group members are entered into a separate table that tracks upstream carriers and call volumes for the Traceback Number. The general process for this effort is highlighted in the below diagram.

[25] 47 USC 222(d)(2).

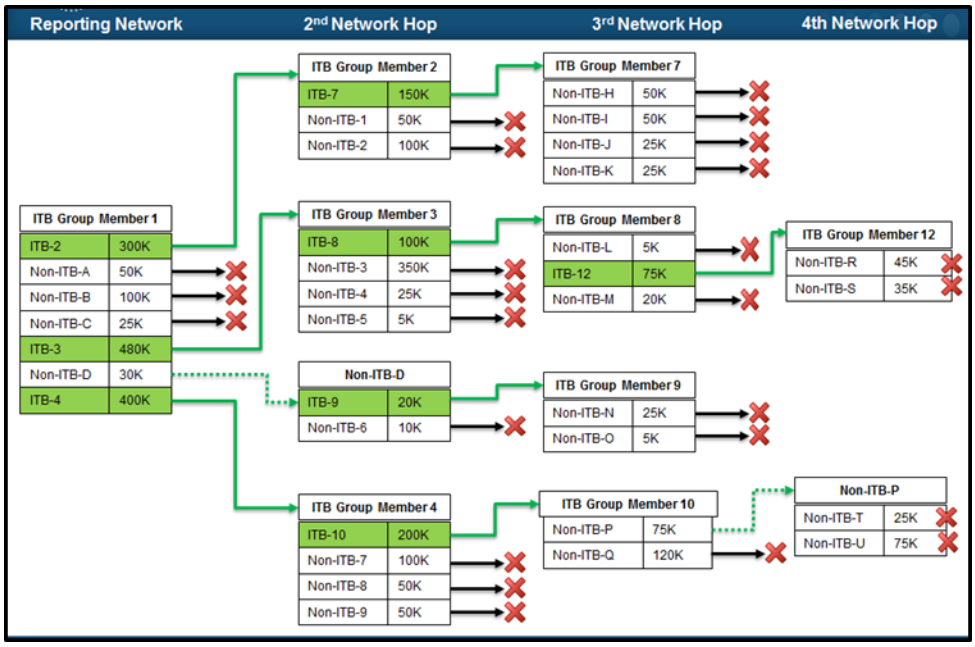


USTelecom will then select an Incident Report from an ITB Group member for an active traceback effort. USTelecom staff coordinates separately with each ITB Group member identified as a source of upstream traffic to obtain the source of their upstream traffic. In addition, USTelecom also reaches out to non-ITB Group members, requesting that the source of their upstream traffic be provided to USTelecom for further traceback efforts. This process is reflected in the below diagram.



This process is repeated through each network hop: USTelecom coordinates with ITB Group members to push back deeper into the network path; while also reaching out to non-ITB Group members requesting additional traceback information. The process continues, until such point that USTelecom can no longer continue to traceback the

Incident Report further into the network path due to the absence of participating ITB Group members and/or non-responsive non-ITB Group members. A sample call path scenario is illustrated below.



In January, 2017, the ITB Group initiated its first traceback effort under the enhanced traceback process. The number at issue involved an IRS-related scam using a non-toll free number. Between January 13, 2017, and January 27, 2017, USTelecom staff identified approximately 70 upstream carriers, and sent approximately forty separate communications to upstream carriers requesting assistance on the ITB Group Traceback efforts (several of these upstream carriers lacked readily available contact information). None of the non-ITB Group members provided actionable information. However, working with just the members of the ITB Group, USTelecom was able to trace the call back through four distinct network hops by the end of the traceback effort.

Finally, USTelecom recently met with staff from the FCC's Enforcement Bureau to discuss the traceback efforts of the ITB Group, and potential handoffs of information collected by the ITB Group during the traceback process. During this initial meeting, USTelecom staff provided FCC personnel with an overview of the enhanced traceback process, discussed areas of potential cooperation, as well as certain challenges faced by industry in these efforts. USTelecom will continue to work with its partners in government and law enforcement, in order to maximize the effectiveness of industry-led efforts.

4.2 USTelecom Status of Do Not Originate Initiatives

On October 26, 2016, USTelecom was directed to complete a report on one component of robocall mitigation efforts known as Do Not Originate (DNO).[26] That report was delivered to Strike Force members on March 31, 2017 (DNO Report). The DNO Report provided an overview of the DNO process, including spoofing challenges associated with this approach, as well as DNO's application as a highly specialized tool. It also included a summary of industry efforts on this issue, including the development of USTelecom's ITB Group, and provided an analysis of three completed DNO trials, and the findings from those efforts. It finally discussed lessons learned over the last two months from these DNO efforts, and provides an analysis on the effectiveness and feasibility of DNO.

This 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 process is implemented, and can be instituted by some or many carriers. Calls from numbers that have been placed on a DNO list are rejected by the first service provider in the call path that has implemented DNO based on the originating telephone number and thus blocked from entering the phone system. This is no substitute for authentication, but USTelecom's testing efforts demonstrated that the process can prevent a certain subset of narrowly defined harmful calls from reaching consumers.

The USTelecom DNO trials demonstrates that applied in a narrow and tightly controlled manner, this can be an effective deterrent in mitigating certain types of large and medium scale attacks. It is important to note that the calls themselves will still route across networks up until the point that the traffic is handed off to a carrier that is instituting a block. Because there are potentially multiple paths for any call to take, the effectiveness of any given effort will rely on the participation rate of carriers. In other words, the more carriers that are instituting a block on a given number, the more effective that particular undertaking will be.

The DNO Report discussed a series of three DNO trials using certain criteria. [27] The three completed trials involved efforts involving the Internal Revenue Service, a toll free directory assistance number, and the Immigration and Customs Enforcement agency. A complete analysis of these efforts was provided to the industry-led Strike Force on March 31, 2017.

4.3 The Effectiveness and Feasibility of DNO.

[26] Id., Section 3.2.3, p. 34.

[27] See e.g., USTelecom Comments, CG Docket No. 02-278, WC Docket No. 02-278, p. 17 (submitted January 23, 2015) (available at: https://ecfsapi.fcc.gov/file/60001015988.pdf) (visited April 22, 2017).

Blocking DNO numbers can be an effective tool for addressing certain types of robocalls (specifically, ones where bad actors spoof known "vanity" numbers to impersonate legitimate callers), when it is applied in a narrow and targeted manner. As USTelecom has previously noted, there is no single 'silver bullet' to the robocall problem,[28] and the process of blocking DNO numbers should be viewed as one of a growing number of tools available to address the robocall problem. In general, robocalls are best addressed in a holistic manner through deployment of a wide variety of tools by a broad range of stakeholders. These stakeholders include consumer groups (e.g., education/awareness, adoption of consumer-based blocking tools), government entities (e.g., enforcement, education, coordination, regulatory protection), standards organizations (e.g., development of industry standards such as SHAKEN/STIR), and industry (e.g., Blocking DNO numbers, traceback, robocall mitigation tools, etc.).

In particular, this process should be paired with robust traceback efforts in order to ensure that the bad actors whose illegal spoofing is being partially mitigated by these policies can be investigated fully and prosecuted if appropriate. As discussed below, the calls that are candidates for the DNO blocking are often among the most egregious legal violations of all categories of robocalls.

USTelecom concludes that the DNO trials outlined in this report were effective due to the efforts being narrowly targeted towards the specific set of telephone numbers identified and confirmed as inbound-only. That is no guarantee that they will be similarly effective in the future, or that they could be successfully scaled without creating harmful unintended consequences. If DNO blocking procedures were more widely deployed beyond a narrow set of numbers (i.e., inbound-only telephone numbers), bad actors could easily and rapidly transition to randomized and/or legitimate telephone numbers in order to circumvent DNO blocks. In fact, the widespread deployment of a broader range of DNO numbers (e.g., unassigned telephone numbers) could have the perverse effect of quickly nullifying any protections, while also making robocallers more difficult to identify. This could also increase instances of both "false positives" (i.e., blocking numbers that should not have been blocked) and "false negatives" (i.e., fail to block numbers that should have been blocked).

Accordingly, due to the nature of the DNO blocking process (i.e., outright blocking in the network), its use should currently be limited to those instances where the number in question (i) is used by bad actors as part of an impersonation scam, (ii) is confirmed as an 'inbound-only' number using strong vetting procedures that go beyond merely asking the subscriber or its carrier about the number's use, and (iii) appropriate authorizations are obtained from the entity to whom the number is assigned. In addition, the process should also be deployed in a highly controlled environment. Carriers must carefully and continually coordinate with the telephone number owner before and during the entire process, in order to ensure that issues arising from inadvertent blocking of legitimate calls

[28] See e.g., USTelecom Comments, CG Docket No. 02-278, WC Docket No. 02-278, p. 17 (submitted January 23, 2015) (available at: https://ecfsapi.fcc.gov/file/60001015988.pdf) (visited April 22, 2017).

do not arise. As happened during one of the trials, legitimate calls will be blocked if any carrier attempts to implement blocks of purported inbound-only numbers without fully vetting the subscriber's understanding that the number is inbound-only.[29] Such false positives should of course be avoided in the first instances, and if they do occur they need to be remedied promptly.

In the near term, any widely deployed efforts would likely face significant technical scalability issues, in addition to the policy risks (e.g. incentivizing more spoofing of legitimate numbers in order to get around DNO blocks) discussed above. For example, the network capabilities for all providers operating in today's voice ecosystem varies widely. In some instances, an individual carrier may even have disparate network capabilities within their respective networks (e.g., portions of the network may be TDM, while other portions may be IP-based). As a result, as any centralized list of DNO numbers grows, it may very well exceed the capacity of certain network systems.

In addition, there is currently no centralized method for obtaining blocking authorizations across the universe of network providers. As a result, letters of authority (LOAs) from each number's owner must ideally be sent to each organization seeking to institute a DNO blocking process, since there is currently no form of 'transitive' authorization. In order to implement DNO blocking process on a broader scale, some form of universal LOA would need to be developed. In addition, some form of centralized distribution method for such LOAs would need to be developed, along with a list management framework. Regarding this latter point, any such list would need to be continually monitored and updated as telephone numbers are added to, or removed from, the list of authorized DNOs, while keeping such information out of nefarious hands.

Because of the risks of unintended consequences if the blocking were implemented in an unmeasured way, USTelecom supports the permissive approach outlined by the Commission in its recent Notice of Proposed Rulemaking.[30] This is an appropriate starting point for considering its applicability to other categories of phone numbers. Specifically, the Commission's proposal is to permit voice service providers to block telephone calls in certain, narrow circumstances to protect subscribers from fraudulent and illegal robocalls. Under the proposal, the Commission would codify the Consumer

[29] Customers who attest that they never initiate calls with a particular number often find other parts of their business, or third parties contracted services, that do. And a carrier that has assigned a number to a customer cannot conclusively and uniquely tell that customer that no other carrier originates traffic using that number to initiate legitimate calls. Outbound services using the telephone number could be hosted in the cloud or third party providers and carried over multiple wholesale provider networks. Given the highly dynamic and competitive call processing and handling ecosystem, which involves a diversity of business arrangements and call center structures, simplistic assumptions about a number's appropriateness for DNO are likely to result in unintended consequences.

[30] See e.g., Blocking NPRM, p. 10 (stating that "it is also important for the Commission to protect the reliability of the nation's communications network and to protect consumers from provider-initiated blocking that harms, rather than helps, consumers. The Commission therefore must balance competing policy considerations – some favoring blocking and others disfavoring blocking – to arrive at an effective solution that maximizes consumer protection and network reliability.").

and Governmental Affairs Bureau guidance public notice that providers may block calls when the subscriber to a particular telephone number requests that calls originating from that number be blocked.[31] USTelecom intends to participate in the Commission's rulemaking proceeding, and it is anticipated that this current report to the Industry Strike Force will help to further inform industry's analysis of this proposal.

4.4. Work with enforcement to shorten the cycle time between identification and action to stop illegal activity

In October 2016, ATIS completed its work on a process to maintain a contact list for robocall related subpoenas as noted by the Initial Strike Force Report. The list is included as part of ATIS' larger service provider contact directory that allows the industry to identify contacts for other key issues, including call termination issues. ATIS maintains this list and has been working to promote the completion of contact information and its use by the industry. ATIS efforts since the Initial Strike Force report include efforts to streamline and automate input processes. This streamlining/automation is expected to be finalized in April 2017.

The ATIS Service Provider Contact Directory is available electronically at no charge. However, because this document is intended only for use only by service provider and enforcement agencies, it is password protected. More information about this document, including how to request the password, is available from: http://www.atis.org/01_committ_forums/NGIIF/contact_directories.asp.

USTelecom also realizes the importance of participation in the ATIS carrier directory. It will continue to coordinate with all of the ITB Group members and the association's individual members to ensure that their updated contact information is added to the list maintained by ATIS. In addition to direct communication and coordination with its individual members and members of the ITB Group, USTelecom has also utilized additional tools to expand awareness of this ATIS effort. These efforts include articles in the association's weekly newsletter, as well as blog entries regarding the importance of the ATIS initiative.

Further, CTIA has ensured that all national carriers have added their contact information to the ATIS service provider contact directory to help expedite investigations into the sources of illegal robocalls.

5. Regulatory Support

[31] The Commission also seeks comment on authorizing providers to block calls from three categories of numbers: invalid numbers, valid numbers that are not allocated to a voice service provider, and valid numbers that are allocated but not assigned to a subscriber.

During the first sixty days, the Strike Force identified several regulatory road blocks and asked the Commission for rule clarifications and, if necessary, rule changes. The Commission addressed those requests in its NPRM and NOI released on March 23, 2017. Industry members expect to comment on the proposed rules and the technical and definitional questions raised by the FCC. Abating illegal robocalls is a complex undertaking, with potential unintended consequences, so carriers must have clear guidelines and protections for actions they may take to facilitate illegal robocall abatement. As new regulatory issues arise, the industry will continue to work with the Commission to remove any additional regulatory road blocks.

6. Conclusion

Significant progress has been made over the past six months. But this is not the end of the industry effort to develop ways to stop unwanted and illegal calls. The industry is committed to continuing to develop mitigation tools and techniques until these illegal harassing calls are stopped.