October 19, 2015

<u>Via Email</u>
Alison Kutler
Acting Bureau Chief
Consumer and Governmental Affairs Bureau
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

**Re: ATIS' Work Programs Related to Caller ID Spoofing, Robocall Mitigation Techniques
Ex Parte, CG Docket No. 02-278, WC Docket No. 07-135, WC Docket No. 13-39**

Dear Ms. Kutler:

The Alliance for Telecommunications Industry Solutions (ATIS) would like to express its appreciation for the opportunity to participate in the September 16, 2015, Commission workshop on robocall blocking and caller ID spoofing. This letter provides additional details regarding ATIS and its work programs relevant to these issues. ATIS also provides comments about other issues raised during the workshop, including the timing of industry work aimed at mitigating the impact of caller ID spoofing and robocalling.

As explained more fully below, ATIS has already initiated an analysis of both the caller ID spoofing and robocalling issues. ATIS will continue to work these efforts and once its initial analysis is complete, will notify the Commission and others of the results. In addition, some of ATIS' members are working to identify commercially available mitigation techniques.

Background

ATIS is a global standards development and technical planning organization that develops technical and operational standards for information, entertainment, and communications technologies. ATIS' diverse membership includes wireless and wireline service providers, equipment manufacturers, broadband providers, software developers, consumer electronics companies, public safety agencies, digital rights management companies, and internet service providers.

ATIS is also one of the founding parties, and sole North American Organizational Partner, to the Third Generation Partnership Project (3GPP), that develops next generation wireless, including Long Term Evolution (LTE), specifications. 3GPP is a global collaborative effort among: ATIS; Association of Radio Industries and Businesses; the China Communications Standards Association; European Telecommunications Standards Institute; Telecommunications Standards Development Society, India; Telecommunications Technology Association; and Telecommunication Technology Committee. ATIS members contribute to the development of 3GPP specifications, which are transposed into ATIS standards for use by the industry in the U.S. and globally.

Composed of senior-level technology experts, ATIS' Technology and Operations (TOPS) Council identifies pressing technical and operational challenges and coordinates the analysis and reports yielding

recommendations for industry-wide solutions. New TOPS Council work programs are initiated to address evolving challenges. Recent initiatives include: Intelligent Programmatic Peering; Reference Functional Model; Testbeds; Public Safety Related Applications; and Integration Platform as a Service.

Technical and operational work in ATIS is completed in ATIS committees and forums. While many of ATIS' committees address issues affecting network reliability and availability, two ATIS committees have particularly relevant work programs: (1) Packet Technologies and Systems Committee (PTSC); and (2) Next Generational Interconnection Interoperability Forum (NGIIF).

ATIS PTSC develops and recommends standards and technical reports related to services, architectures, and signaling. PTSC's work programs focus on issues such as Emergency Telecommunications Service (ETS), cybersecurity, IP-to-IP interconnection, lawfully-authorized electronic surveillance and the evolution of the PSTN. PTSC's work program associated with caller ID spoofing is taking place primarily within its Cybersecurity (PTSC CSEC) Subcommittee, which is developing implementable security standards relevant to packet-based telecommunications networks, maintaining and further developing the cybersecurity reference architecture developed by the ATIS Cybersecurity Focus Group, addressing the impact of government regulations and requests by government agencies, and assessing new cybersecurity issues that arise.

PTSC is also the primary consensus body within ATIS that is working collaboratively with the SIP Forum on the development of voluntary IP network-to-network (NNI) specifications that will promote communications interoperability, competition and innovation. In 2015, ATIS and the SIP Forum published the first standardized IP-based NNI interconnection with consensus across North American service providers. The next phase of this joint work effort, currently underway, is expected to address inter-carrier video calling and enhanced calling name delivery (CNAM), and to include an implementation profile for secure caller ID.

ATIS NGIIF provides an open forum to encourage the discussion and resolution of industry-wide issues associated with the operational aspect of telecommunications network interconnection and interoperability, and the exchange of information concerning relevant topics, such as network architecture, management, testing and operations, and facilities. This input addresses, and is used to develop, operational procedures associated with these emerging technologies as well as next-generation network interconnection and interoperability issues that involve architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators.

ATIS Work Programs Related to Caller ID Spoofing and Robocalls

ATIS Technical Report on Originating Party Spoofing in IP Communication Networks. PTSC has an active work program aimed at addressing caller ID spoofing events in IP networks. Noting that spoofing of the originating (calling party) identity is used for such potentially malicious activities as vishing, robocalling, swatting, anonymity breaking, etc., the PTSC CSEC is developing a technical report that will review problems associated with originating party spoofing in IP communication networks and analyze mitigation techniques to better assess their applicability in the converged IP communication network environment. Among the mitigation techniques that are being evaluated are:

- 3GPP P-Asserted-Identity (PAI) trust model;

- ATIS Verified Token (summarized more below);
- Signing parts of SIP messages based on RFC 4474bis within the proposed Internet Engineering Task Force (IETF) Secure Telephone Identity Revisited (STIR);
- Blacklists (local and global);
- Whitelists (local and global);
- Honey Pots;
- Post call notification (e.g., dial a "*" code after hanging up); and
- Network Verification of SIP PAI/FROM for IP PBX call originations.

The target completion date of this technical report is early 2016.

ATIS/SIP Forum Verified Token Mitigation Technique. ATIS and its PTSC are working with the SIP Forum on the development of a specification for an extensible canonical token (Verified Token) that cryptographically represents the originating calling number and the provider that originated the call. The objective of the Verified Token technique is to incorporate a separable and evolutionary approach that offers carrier-based validation. While the effectiveness of the Verified Token technique is not yet fully understood given its limited coverage of IP-to-IP domestically originated/terminated calls, known advantages of this approach include:

- Fewer certificates would be needed (a few thousand certificates in a carrier-based alternative vs. many millions in a per- telephone number approach), requiring less complex certificate issuance and revocation infrastructure; and
- The existing telephone number validation, assignment, and porting infrastructure can remain in place, eliminating the need to create/maintain parallel infrastructure during the all-IP transition.

This mitigation technique has been provided to the IETF on an informational basis for feedback.

The ATIS TOPS Council and NGIIF are also examining the ATIS/SIP Forum Verified Token proposal, and the related IETF STIR approach, from other perspectives. The TOPS Council is developing use and test cases to evaluate the Verified Token and the IETF STIR approaches. These use and test cases will be essential to the testing of these mitigation techniques. However, significant additional industry work will be required before equipment testing could be performed. NGIIF is also reviewing both approaches with a longer-term goal of identifying operational impacts and developing best practices.

Operational Strategies to Mitigate the Impact of Caller ID Spoofing and Enhance the Integrity of Caller ID Services. ATIS NGIIF is developing a baseline document that discusses caller ID spoofing issues and methodologies to mitigate the impact of inappropriate caller ID spoofing for the purpose offering operational strategies that enhance the integrity of caller ID services. This work program, which is expected to be completed in 2016, will examine types of caller ID services, examples of caller ID spoofing and the use of auto dialers for purposes such as telemarketing, public service and/or political messages, and security. The deliverable will also address the need to maintain the integrity of caller ID services, the impact of caller ID spoofing and relevant regulatory issues.

Other Relevant Work Programs. ATIS NGIIF has published a number of documents that are also relevant to the examination of caller ID spoofing and robocalling. For example:

- *Best Practices for Emergency Notification System (ENS) Call Volume Testing Procedure: Wireline* (ATIS-0300098) addresses the optimization of call completion between telecommunications or VoIP service providers and ENS users or initiators. This document outlines the testing process for

ENS users or initiators and the corresponding service provider when using the PSTN for the delivery of ENS calls.

- *NGIIF Auto Dialers Reference Document - Auto Dialers Basics* (ATIS-0300105) provides basic information regarding the use of auto dialers. Robocalling is classified as a form of an auto dialer service, and is discussed in greater detail in the document. This document explains how auto dialers are used and their potential impacts on service provider networks (wireline, wireless, TDM and VoIP). The document also illustrates how to: differentiate between legitimate auto dialer calls and those calls that may be associated with potentially illegal activities; and assess the risk and impact on the network, ENS, the industry, and consumers.
- The ATIS TOPS Council recently launched a landscape study to examine industry anti-spoofing activities currently underway and document how these relate to "use cases" that characterize the full range of network technology and call origin scenarios.
- While not an ATIS work program, ATIS and NGIIF member companies provided input on another relevant document, *Best Practices to Address Online, Mobile, and Telephony Threats*. This document was prepared June 1, 2015, by the Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) and London Action Plan and addresses, among other things, best practices to combat robocalls and caller ID spoofing.

3GPP Study on IMS Enhanced Spoofed Call Prevention and Detection. As the North American partner of 3GPP, ATIS and its members are also contributing to the ongoing 3GPP work program that is examining enhanced prevention and detection of caller ID spoofing as it relates to IP Multimedia Subsystem (IMS). IMS, an all-IP system designed to assist mobile operators deliver next generation interactive and interoperable services, has been adopted by other industry sectors, including wireline and cable industries. The 3GPP work program under development will, among other things, examine IETF STIR to determine what aspects should be recommended for incorporation into 3GPP IMS security specifications. The program is also looking at other service interaction and deployment scenarios, including roaming, business line trunking, and circuit switched to IMS transitions.

ATIS Comments on Timeline and Other Issues

ATIS notes that, as part of the workshop agenda, an aspirational timeline of industry work was provided. While ATIS appreciates the Commission's work to promote industry solutions, it has some high-level input regarding this timeline and other related issues:

- ATIS has concerns that it is not possible to meet all of the dates in the proposed timeline. Even for the carrier-based certificate (i.e., Verified Token) approach described above, the timeline is aggressive.
- The timeline suggests that all VoIP-originated calls would be signed by summer of 2017. It should be noted that this is not the last step needed to implement mitigation techniques and that further implementation steps (e.g., network equipment vendors, manufacturers) would require additional time beyond this date.
- Until such standards and best practices are fully defined and operational capabilities have been made available to service providers by the vendor community, ATIS believes that it is premature to speculate on the feasibility of adopting or implementing specific standards or best practices. For this same reason, singling out any one specific mitigation technique in the timeline may also be premature.

- Any discussion of timelines only makes sense in the context of a specific mitigation technique. Different techniques may have different timelines associated with them. For example, the timeline includes a mix of "carrier-based" and "telephone number-based" certificate deliverables; the timelines associated with these two types of deliverables should be considered separately.

- ATIS urges the Commission to allow the industry time to work the technical issues before considering any regulatory action. Some service providers already provide certain mitigation techniques to their customers. However, additional time would be required to potentially facilitate the ubiquitous deployment of one or more techniques. Commission action could introduce delays in the technical work as companies may become more circumspect when working technical issues that are the subject of an ongoing rulemaking.

- The caller ID/robocalling issue is complex and there is no "silver bullet." No caller ID validation or anti-spoofing approach can address all aspects of this problem. As a result, it is better to talk about "mitigation techniques" rather than "solutions" and to refrain from providing assurances regarding the techniques' effectiveness or any noticeable impact consumers may reasonably expect in the near future. The industry will need a layered approach that will use a variety of mitigation techniques.

- Mitigation techniques need to be evaluated based on their potential efficacy. The industry's focus has been on IP-based mitigation techniques as there is no mitigation technique that can be reasonably implemented to effectively address caller ID spoofing for circuit switched originating and terminating calls.

- The Commission should be sensitive to the fact that bad actors will also be examining regulatory and technical changes (i.e., as mitigation techniques evolve, so too will the tools used to evade these techniques). The effort to address caller ID spoofing and robocalls will be an ongoing industry effort with new/updated mitigation techniques being examined, tested and deployed to address evolving threats.

- The global nature of caller ID spoofing and robocalls also presents challenges for the industry. For example, verifying the caller ID for calls originating outside of the U.S. is inherently problematic. Another challenge arises because some countries, including the U.S., permit the use of caller ID spoofing in certain circumstances, which makes it difficult to distinguish between legitimate and illegal spoofed calls in certain call use-case scenarios.

- As there may be no way to differentiate between incomplete calls to rural areas and calls blocked at the request of rural end-users, the call completion statistics required by the November 8, 2013, *Report and Order* in WC Docket No 13-39 could be affected. The Commission may wish to consider whether changes to its call completion recording, retention and reporting requirements would be warranted to acknowledge service providers' efforts to offer mitigation techniques to its customers. It is vital that mitigation efforts be handled with care, so that the reliability of the PSTN is not compromised.

- Finally, ATIS notes that there is a critical need for a "safe harbor" that would protect carriers from liability associated with blocked calls.

ATIS's input above is focused on the timeline as it relates to the development of a preliminary list of targeted ATIS specifications/best practices. ATIS is not providing input on the activities in the timeline that suggest steps to be taken by service providers and vendors to implement these specifications/best practices nor on the costs/benefits associated with doing so. ATIS is also not providing input on interdependencies to implementation of specific specifications/best practices that will determine

effectiveness, or issues outside of the control of service providers or classes of service providers, including other significant challenges they might face based on their technology, network, customer-base, services, or other factors. In addition, ATIS work is generally focused on calls originating from and/or terminating to domestic U.S. service providers.

ATIS recognizes that it is not the only stakeholder in this effort. ATIS looks forward to working even more closely with IETF and others and notes that further input from these stakeholders on the timeline, feasibility, cost/benefit, and barriers will be essential.

ATIS would welcome the Commission encouraging non-traditional stakeholders to participate in ongoing industry efforts to evaluate technical challenges. ATIS would also welcome working with non-traditional stakeholders and its own membership to provide written updates to the Commission and participate through joint periodic calls/meetings so that other stakeholders and ATIS can together provide relevant updates and allow the Commission to provide input and ask questions.

If you have any questions or need more information, please do not hesitate to contact the undersigned.

Sincerely,

Thomas Goode
ATIS, General Counsel

cc: Chairman Tom Wheeler
        Commissioner Mignon Clyburn
        Commissioner Jessica Rosenworcel
        Commissioner Ajit Pai
        Commissioner Michael O'Rielly
        Mark Stone, Deputy Bureau Chief
        Kurt Schroeder, Chief, Consumer Policy Division and Information Access and Privacy Office
        John B. Adams, Deputy Chief, Consumer Policy Division &Information Access & Privacy Office
        Kristi Thornton, Attorney
        Christina Clearwater, Attorney Advisor
        Martin Dolly, PTSC Chair
        Viqar Shaikh, PTSC Vice-Chair
        Amy Hindman, NGIIF Co-Chair
        Mary Retka, NGIIF Co-Chair