In the Matter of	)	
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	
	)	

COMMENTS OF THE ALLIANCE
FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS

Thomas Goode
General Counsel
ATIS
1200 G Street, NW
Suite 500
Washington, DC 20005
(202) 628-6380

August 14, 2017

TABLE OF CONTENTS

SUMMARY

ATIS is pleased to have the opportunity to respond to the comments in this proceeding. As the Commission is well aware, ATIS has been involved with call authentication and the effects of robocalling for many years and has been a key force and a major architect in the development of the Signature-based Handling of Asserted information using toKENs (SHAKEN) framework. While ATIS supports the Commission's examination of important call authentication issues, it notes that there is significant industry work underway and urges the Commission to allow the industry to complete this work before making any decisions regarding the call authentication trust anchor.

ATIS does not believe that further regulatory action by the Commission to promote the adoption and implementation of authentication frameworks is necessary at this time because market forces are sufficient to encourage the continued adoption of call authentication frameworks. Nor does ATIS believe that there are any existing laws and regulations that would prevent the deployment of SHAKEN nor impede the ability of service providers (or call blocking services) to use SHAKEN once implemented. ATIS also cautions that the incorporation of new approaches or new variations to SHAKEN/Secure Telephone Identity Revisited (STIR) at this late stage may introduce confusion and delay implementation progress.

ATIS has been working with the industry to identify an effective call authentication governance authority structure. Under ATIS' proposed structure, the governance authority would be established and operated by the industry under the umbrella of a multi-stakeholder industry organization. ATIS maintains that the governance authority and policy administrator would require different expertise that may warrant performance of these roles by separate entities and further recommends that an RFP-type process be used to identify the appropriate policy administrator. ATIS stands ready to assist the industry by serving as the governance authority.

ATIS supports the use of an Operating Company Number (OCN) as the criteria for receiving SHAKEN certificates, as well as the use of the ACME protocol for communicating with certification authorities. However, ATIS notes that SHAKEN does not prohibit the use of other certificate distribution protocols. ATIS also does not believe that the implementation of SHAKEN by the industry will create unique privacy concerns and notes that the industry has taken steps to address privacy issues in its development of SHAKEN.

Finally, ATIS recommends that a stable funding mechanism be identified that allows costs to be distributed equitably, and is flexible and reviewed periodically.

In the Matter of	)	
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	
	)	

COMMENTS OF THE ALLIANCE FOR
TELECOMMUNICATIONS INDUSTRY SOLUTIONS

The Alliance for Telecommunications Industry Solutions (ATIS), hereby submits these

comments in response to the *Notice of Inquiry* (*NOI*), released July 14, 2017, in the above-

referenced docket. As a key stakeholder in the development of technical and operational

standards pertaining to unlawful robocalling, ATIS is pleased to have the opportunity to respond

to the comments in this proceeding. While ATIS supports the Commission's examination of

important call authentication issues, it notes that there is significant industry work underway and

urges the Commission to allow the industry to complete this work before making any decisions

regarding the call authentication trust anchor. ATIS stands willing to assist the industry in

advancing the call authentication ecosystem by serving as the governance authority.

I.   BACKGROUND

ATIS is a global standards development and technical planning organization that

develops and promotes worldwide technical and operations standards for the technology

information, entertainment, and communications industries. ATIS' nearly 200 member

companies are currently working to address 5G, cybersecurity, the All-IP transition, network

functions virtualization, smart cities, IoT, emergency services, the network's evolution to

content-optimized networks, quality of service, billing support, operations, unmanned aerial

vehicles, and much more. ATIS is accredited by the American National Standards Institute

(ANSI) and is the North American Organizational Partner for the 3rd Generation Partnership

Project (3GPP), 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 appreciates the opportunity to provide feedback on this important issue. As the

Commission is well-aware, ATIS has been involved with call authentication and the effects of

robocalling for many years and has been a key force and a major architect in the development of

the SHAKEN framework. This current work program has three phases:

- Phase 1: Publication of the Signature-based Handling of Asserted Information Using toKENs (SHAKEN)[1] technical specification that describes how calls may be authenticated by service providers (January 2017).

- Phase 2: Publication of the Signature-Based Handling of Asserted Information Using Tokens (SHAKEN): Governance Model And Certificate Management (Governance Model)[2] that describes how SHAKEN could be operationalized by the industry, including the need for a governance authority[3] and policy administrator (July 2017);[4] and

- Phase 3: Publication of deliverables to address call display issues, implementation guidance/best practices, deployment metrics and to further detail the operation of the policy administrator (estimated completion date 4th quarter 2017).[5]

---

[1] This document is available at no charge from http://www.atis.org/01_resources/whitepapers.asp.
[2] This document is available at no charge from http://www.atis.org/01_resources/whitepapers.asp.
[3] Referred to in the *SHAKEN Governance Model* as the Secure Telephone Identity Governance Authority or STI-GA.
[4] Referred to in the *SHAKEN Governance Model* as STI Policy Administrator or STI-PA.
[5] This activity also includes efforts to continue industry testing of SHAKEN implementations through efforts such as the ATIS Robocalling Testbed.

Because this third phase of work is currently underway and expected to be completed by the end of the year, ATIS strongly urges the Commission to not take any action on this matter until the industry has completed its on-going work. ATIS continues to believe that the industry is best positioned to progress this work and that premature action by the Commission could serve to disrupt and/or significantly delay the industry's progress and the target delivery of this work.

II. COMMENTS

A. Promoting Implementation of Call Authentication Tools

In the *NOI*, the Commission seeks comment on what it should do, if anything, to promote the adoption and implementation of authentication frameworks, including the SHAKEN and STIR frameworks.[6] ATIS does not believe that further regulatory action by the Commission is necessary at this time because market forces are sufficient to encourage the continued adoption of SHAKEN. In fact, ATIS notes that key service providers are already moving aggressively to enable the deployment of SHAKEN, similar to the way that the industry worked without a mandate to deploy caller ID. Service providers are already highly incented to provide call authentication to meet the needs of consumers in the competitive marketplace; regulatory mandates are therefore unnecessary.[7]

While ATIS does not see a need for new regulatory mandates, it does believe that there is are strong roles for the Commission to play in: (1) helping the industry to educate consumers on the availability of new call authentication tools; (2) educating service providers, large and small, on the availability of these new tools; and (3) continuing enforcement efforts against bad actors.

The Commission asks about the relevant time frames or milestones that should be

---

[6] *NOI* at ¶14.
[7] However, ATIS recognizes that this is a complex dynamic, and that it may be appropriate for the FCC to continue to monitor deployment of SHAKEN.

considered associated with any Commission action to promote the implementation of authentication frameworks.[8] As ATIS maintains that no Commission action is necessary to promote adoption and implementation of SHAKEN, ATIS does not believe that time frames or milestones should be established by the Commission. ATIS further notes that work is underway within ATIS' Packet Technologies and Systems Committee (PTSC) and the ATIS/SIP Forum IP-NNI Task Force to identify deployment metrics, best practices for SHAKEN deployment, and operational and management considerations for SHAKEN STI Certification Authorities that are expected to be completed by the end of 2017. ATIS believes and recommends that the industry should be permitted to complete this work before any decisions regarding timelines or milestones are made.

The Commission also seeks input regarding any existing laws, regulations, market failures, or other factors that would prevent or discourage stakeholders from developing, implementing, or deploying authentication frameworks.[9] ATIS does not believe that there are any existing laws and regulations that would prevent the deployment of SHAKEN or impede the ability of service providers (or call blocking services) to use SHAKEN once implemented. However, ATIS acknowledges that unforeseen questions or issues could arise post-deployment.

As explained more fully below, ATIS recommends that the governance authority be tasked with identifying emerging issues related to the deployment of SHAKEN to determine, identify, and address future impediments, including best practices that may be considered by the industry. This effort may also include identifying a need for a safe harbor provision to cover and

---

[8] *NOI* at ¶15.
[9] *NOI* at ¶16.

protect service providers deploying SHAKEN and associated call blocking services if following recognized best practices.

B. Alternatives to SHAKEN/STIR

The availability of viable alternatives to, or variants of, SHAKEN and the STIR is also discussed in the *NOI*.[10] SHAKEN and STIR are the only open, standardized mechanisms for call authentication that are supported as practical and deployable by the industry. While some vendor-specific variants/alternatives have been discussed, these have not been fully vetted by the industry. ATIS believes that incorporation of new approaches or new variations to SHAKEN/STIR at this late stage may only introduce confusion and delay implementation progress. ATIS urges the Commission not to disrupt the industry's work on this matter by proposing variations to SHAKEN/STIR.

The Commission also asks for input on alternative means of call authentication, noting that some X.509 systems lack a centralized governance authority or policy administrator and, instead, allow end users' systems to rely upon the reputation of multiple competing self-certifying certification authorities.[11] ATIS believes that a decentralized X.509 model would not be as effective as the model envisioned in SHAKEN, particularly in the near term. The fundamental underlying principle behind SHAKEN is to create a single authoritative governance authority (per country) and to restrict participation to entities that can be trusted. ATIS maintains this is a much more "deployable" and effective approach than one allowing competing, self-certifying, systems. Moreover, ATIS believes the impact to consumers, as evidenced by the significant number of robocall-related consumer complaints that the Commission receives each

---

[10] *NOI* at ¶17.
[11] *NOI* at ¶25.

year, warrants a systematic approach to ensure consistency in addressing this issue. The

SHAKEN centralized approach ensures that calls can be reliably signed and that, when a call is

signed, the information is accurate. This approach also can enable other complementary

functions, such as analytics services (e.g., call blocking apps), which can use the information

provided by SHAKEN, along with information from other sources, to reliably identify robocalls

and based on consumer choices, potentially block these calls.

C. Creation of an Integrated SS7/SIP Authentication Framework

Noting that SHAKEN/STIR applies only to SIP-based systems, the Commission also

seeks comment on the benefits and viability of creating an integrated authentication framework

across both IP and older TDM systems.[12] ATIS does not believe that the creation of an

authentication framework for SS7 and other legacy technologies is feasible. Not only would

such an undertaking be extremely costly and complex, it would be particularly challenging given

that most SS7/TDM equipment has been discontinued and some manufacturers have left the

marketplace.

Attempting to create an integrated framework also would add complexity to the SIP-

based solution that the industry is implementing and these complexities would likely persist long

after the remaining SS7 equipment was retired. Furthermore, it would delay implementation of

SHAKEN and force the industry to rework this issue, creating the possibility that TDM

equipment would be retired before an integrated framework could be developed or deployed.

ATIS also submits that given the continuing evolution of communications networks to

SIP, there may be relatively little return on the significant costs/delays associated with the

---

[12] *NOI* at ¶39.

development of an integrated system. And while the number of SS7 networks has declined, the

number of SIP-based networks for which SHAKEN could apply is rapidly growing, including all

voice over LTE (VoLTE) systems and most cable networks. ATIS, therefore, urges the

Commission not to unnecessarily delay the availability of SHAKEN by mandating the creation

of an integrated authentication framework for both SIP- and SS7-based networks. Instead, the

Commission should allow the industry to move ahead with its forward-looking, deployable, and

implementable approach.

ATIS recognizes that bad actors will continue to use the existing SS7 networks to work

around the SHAKEN call authentication framework. The challenges associated with this

problem will remain an issue that the governance authority, working with industry, will need to

address.

D. Governance Authority and Policy Administrator

The Commission seeks input on a number of issues related to the governance authority

and policy administrator, including what entities would best perform these roles, how these two

roles interact, and whether both functions can be performed by a single entity.[13] As noted above,

the industry is still working to better define the roles and responsibilities associated with the call

authentication ecosystem.

ATIS, in line with the its commitments made to the industry's Robocalling Strike Force,

has been working with the industry to identify a governance authority structure that it believes

would be an effective model.[14] Under ATIS' proposed structure, the governance authority would

---

[13] *NOI* at ¶¶18-27.
[14] ATIS met with the Commission on June 28, 2017, to provide an update on the industry's work on this matter. See ATIS' ex parte presentation in CG Docket No. 17-59, June 30, 2017. These comments build upon and provide further detail regarding the principles outlined in that presentation.

be established and operated by the industry under the umbrella of a multi-stakeholder industry organization such as ATIS. The governance authority would, using consensus-based, open and transparent procedures, define the policies and procedures governing which entities can acquire Secure Telephone Identity (STI) certificates as well as which entities can manage the Public Key Infrastructure (PKI) and issue STI certificates. These policies and procedures would be amended based on actual deployment experience and the response of malicious entities. The governance authority would include broad participation from stakeholders, leverage industry technical expertise to analyze what is happening "in the field," identify emerging issues, and propose timely modifications to the rules to address potential gaps before they become major issues. A multi-stakeholder, industry-based, consensus-driven organization may also provide an effective and timely feedback mechanism to ensure the industry can respond to new robocalling challenges. ATIS maintains that flexibility and speed will be critical factors in addressing challenges posed by bad actors that are constantly refining and evolving their techniques.

ATIS stands ready to assist the industry with the implementation of SHAKEN by serving as the governance authority. ATIS has proven experience managing complex projects using open, consensus-based and equitable processes, and encouraging participation from all segments of the industry. As a trusted, neutral technically-focused organization, ATIS can ensure that the governance authority can resolve issues fairly. ATIS also has significant experience with call authentication issues, having developed technical and operational standards to mitigate the impacts of robocalling and caller ID spoofing issues for many years. ATIS also has been heavily involved in the industry's Robocalling Strike Force and was a key driver in the development of SHAKEN. This familiarity would allow ATIS to address technical issues and/or make modifications to SHAKEN as necessary to address new call authentication challenges.

Two examples of this recommended industry-led structure already exist within ATIS. The Administrative Council for Terminal Attachments (ACTA), jointly sponsored by ATIS and the Telecommunications Industry Association, adopts technical criteria for terminal equipment to prevent harm to the public switched telephone network (PSTN) (as defined in 47 C.F.R. § 68.3) and establishes and maintains database(s) of equipment approved as compliant with this technical criteria.[15] ACTA is a non-governmental, telecommunications industry-directed entity representing all segments of the industry using fair, balanced and open procedures. While enforcement of the underlying Part 68 rules remains with the Commission, the industry manages the adoption of new technical criteria, and maintains rules and procedures for the registration of compliant equipment. This approach has allowed the ACTA to update the technical criteria as appropriate, quickly answer inquiries pertaining to the Part 68 database, and adopt new procedures to streamline equipment registrations.

Another example of this type of structure can be seen in the ATIS IMSI Oversight Committee (IOC), which oversees the management of IMSI codes that have been assigned to the United States and its possessions, as authorized by the U.S. Department of State.[16] The IOC develops and approves guidelines and procedures related to the assignment of IMSIs, which are used to identify subscribers and essential to permit roaming on LTE wireless networks. The IOC permits broad participation and works by consensus. This flexible approach allows the industry to modify the guidelines/procedures to address evolving industry needs without the need for cumbersome regulatory processes. When, for example, FirstNet was established and changes to the assignment guidelines were requested to allow the assignment of IMSIs for the FirstNet nationwide LTE network, the IOC was able to quickly address this request without the time and

---

[15] For more information on ACTA, please see www.part68.org.
[16] For more information on ATIS IOC, please see www.atis.org/01_committ_forums/IOC/.

effort that would have been involved if the assignment of IMSIs were under the direct control of the Commission.

Additionally, while the SHAKEN governance authority and policy administrator could be a single entity, ATIS believes that the roles these entities are envisioned to play are distinct. Each require different expertise such that trying to combine these two roles into one entity may unnecessarily complicate the call authentication ecosystem. The policy administrator is an operational entity that requires expertise and experience with efficiently executing well-defined processes, while the governance authority requires expertise and experience with overseeing the development and maintenance of equitable processes and with fairly applying and modifying processes as needed to address evolving needs. Separating these two roles would also allow the industry to have a greater role in overseeing the policy administrator through participation in the governance authority.

The Commission seeks comment on what qualifications an entity must have to serve effectively as policy administrator and effectively perform certain governance authority roles, either independently, or at the direction of the Commission.[17] As noted above, ATIS believes that the governance authority and policy administrator each require different expertise that may warrant these two roles being performed by separate entities. In terms of qualifications for the policy administrator role, ATIS notes that in addition to expertise and experience with efficiently executing well-defined processes, an entity performing this role should also have experience managing industry resources, such as numbering databases. It would also be beneficial if the policy administrator has significant telecommunications industry and/or certificate management experience. Knowing how the industry operates and having experience with managing industry

---

[17] *NOI* at ¶19.

resources would be beneficial because, as noted in the *SHAKEN Governance Model*, the policy administrator's role would include: (1) implementing policies established by the governance authority, including policies to confirm that service providers are authorized to request certificates and to authorize the certification authority to issue STI certificates; (2) managing an active, secure list of approved certification authorities in the form of their public key certificates and provide this list to the service provider; and (3) maintaining a distinct PKI for digitally signing service provider code tokens.[18] Because the industry is currently working to provide additional details regarding the policy administrator role, ATIS recommends that the Commission not adopt any rules pertaining to this matter until after the industry has completed its work.

The Commission also asks for comment on whether it could designate an existing numbering administrator, such as the North American Numbering Plan Administrator, Pooling Administrator or Local Number Portability Administrator, as the policy administrator for call authentication.[19] While ATIS believes that an existing number administrator may have some of the expertise to serve as the policy administrator, the role envisioned for the call authentication policy administrator is significantly different than other existing databases or programs such that there may not be significant advantages to this approach. Instead, ATIS recommends an RFP-type process be used to identify the appropriate policy administrator. This process could be overseen by the governance authority. In either scenario, there will be a need for a transparent

---

[18] SHAKEN Governance Model, section 5.2.1. The Commission in the *NOI* also asks whether there would be an impact on qualification were certificates issued for specific telephone numbers (or number blocks) rather than for each service provider as proposed in the Governance Model. (*NOI* at ¶19) ATIS does not believe that the overall qualifications would change but adding this complexity may require additional expertise with large-scale resource management.

[19] *NOI* at ¶21.

process that allows for the expeditious selection of a policy administrator. The ongoing industry work to further define the policy administrator role will be useful in developing this RFP.

Finally on this topic, the FCC seeks comment on how the governance authority and the policy administrator should develop, amend, and implement the criteria for selecting certification authorities, designating service providers, and determining certificate coverage.[20] ATIS maintains that an industry-led governance authority, with participation by all stakeholders, is the most effective way to evolve the criteria for selecting certification authorities and "service providers" entitled to obtain STI certificates. As the governance authority, ATIS would establish processes to facilitate broad participation from all key stakeholders, including service providers, equipment vendors, and call blocking services that will use SHAKEN verification information.

E. Certification Authorities

In the *NOI*, the Commission asks for input regarding industry-recommended criteria for certification authorities, namely that they have: (1) sufficient certificate management expertise; and (2) an in-market presence (i.e., being incorporated in the United States).[21] While these two criteria were removed from the *SHAKEN Governance Model*, ATIS supports these criteria. These criteria are important in ensuring that the new call authentication tools can be rolled out seamlessly based on the needs of U.S. consumers. ATIS notes that the industry's phase 3 work, as described above, includes an initiative by the ATIS/SIP Forum Joint IP-NNI Task Force to provide additional details on the operation of the policy administrator. This deliverable, which is

---

[20] *NOI* at ¶32.
[21] *NOI* at ¶29.

expected to be completed later this year, will provide appropriate guidance on criteria for the policy administrator role.

The Commission continues on this same topic to ask whether there are existing entities that are likely to be appropriate certification authorities, such as numbering-related entities like the NANPA, Pooling Administrator, or LNPA.[22] ATIS believes that there may be some confusion regarding the policy administrator and certification authority roles. The *SHAKEN Governance Model* envisions that the certification function is separate and distinct from both the governance authority and the policy administrator. Unlike the governance authority, which defines the policies and procedures governing which entities can acquire STI certificates, and the policy administrator, which confirms that service providers are authorized to request STI certificates, certification authorities are commercial entities that actually issue digital certificates.[23] Furthermore, unlike the governance authority and policy administrator, there is no designated, centralized certification authority in SHAKEN. There will likely be a number of these entities in the U.S. and service providers may decide to establish an internal certification authority. ATIS does not believe that it would be appropriate for the Commission to assign this function to any particular entity.

F. Service Provider Eligibility

The Commission notes that the *SHAKEN Governance Model* proposes that service providers must have an Operating Company Number (OCN) in order to sign calling party information.[24] ATIS supports the use of an OCN as the criteria for receiving SHAKEN

---

[22] *NOI* at ¶¶20-24.
[23] *SHAKEN Governance Model*, Sections 5.2, 5.2.1 and 5.2.2.
[24] *NOI* at ¶30.

certificates, believing this to a reliable and clear criteria for the initial deployment of SHAKEN

that will help to prevent bad (or careless) actors from undermining the system. However, ATIS

acknowledges that there may be unique cases that could be considered in which different criteria

may be appropriate. ATIS maintains that the governance authority will be able to better identify

and address other legitimate criteria once the industry gains operational experience with

SHAKEN. To do this, ATIS believes that the governance authority will need to have broad

industry participation and the authority to revise the criteria for issuing STI certificates to address

evolving needs and threats.

G. Scope of Certificate Coverage

The Commission in the *NOI* asks for input on the assumption in SHAKEN that

certificates will cover particular service providers, noting that certificates can alternatively cover

specific telephone numbers or ranges of telephone numbers.[25] ATIS supports having certificates

covering service providers and believes that this approach will avoid the unnecessary costs and

complexities associated with issuing certificates for individual telephone numbers or ranges of

numbers. ATIS is concerned that trying to add too many new features to SHAKEN will increase

the risk that these changes could create implementation challenges, particularly given that the

industry is building a new ecosystem with SHAKEN. Adding new complexities to an already

challenging task is not a good idea. It is better in ATIS' view to start with a simple framework

that is more easily implementable but that can be modified in time by the industry.[26]

---

[25] *NOI* at ¶31.

[26] The ATIS/SIP Forum Joint IP-NNI Task Force is investigating mechanisms that would allow support enterprise use cases that are similar to the per-telephone number approach referenced in the *NOI*.

H. Use of ACME

The Commission notes that SHAKEN specifies that service providers will communicate with certification authorities using a specific secure, automated protocol called ACME and seeks comment on this aspect of SHAKEN.[27] ATIS notes that SHAKEN focuses on ACME because the industry views this as the most future-proof protocol option. However, it is not correct to say that SHAKEN requires use of ACME. SHAKEN does not prohibit the use of other certificate distribution protocols and, in fact, Appendix A of the *SHAKEN Governance Model* provides an example of how OpenSSL could be used to request SHAKEN certificates.[28] ATIS believes that other protocols could be considered by the governance authority as either interim or permanent options.

I. Valid Types of Call Authentication Verification/Authentication Providers

The *NOI* notes that SHAKEN and STIR presume that large service providers and third party proxies serving smaller providers will be the typical entities conducting call authentication and verification, and asks about the potential costs and benefits of allowing different types of entities and devices to provide authentication and verification services.[29] ATIS believes that expanding the types of providers that provide authentication beyond service providers and third party proxies at this juncture would needlessly complicate and increase the costs associated with the implementation of SHAKEN and STIR.

A key focus of the industry's work on SHAKEN has been to develop a solution that can be deployed near-term and ATIS believes that the Commission should avoid taking actions that

---

[27] *NOI* at ¶36.
[28] *SHAKEN Governance Model*, Appendix A – Certificate Creation & Validation with OpenSSL.
[29] *NOI* at ¶35.

would could delay the near-term implementation of SHAKEN. However, the industry

recognizes that there will be a continuing need to examine SHAKEN to determine if

enhancements are needed to address evolving capabilities and threats. Therefore, while ATIS

believes that it is premature to consider per device authentication/certificates at this point, it

notes that this functionality could be added at some point in the future if the industry finds it

desirable and feasible to do so. Ensuring this flexibility to evolve call authentication to meet

future needs is why ATIS worked with the Internet Engineering Task Force (IETF) to merge

SHAKEN and STIR, and why the industry supports an industry-led, consensus-based

governance authority with representation from all relevant stakeholders

J. Impact on International Calling

The Commission seeks comment on the effects of an authentication framework on

spoofing and robocalls originating in other countries, as well as potential unintended effects on

other types of international calling.[30] ATIS notes that one potential impact from the

implementation of call authentication tools such as SHAKEN is that it may change how bad

operators operate. As SHAKEN is implemented in the U.S., bad actors will likely stop using

VoIP gateways into SIP networks because these gateways could be signed with a unique OrigID

that would identify the calls as international traffic. Instead, these bad actors may attempt to use

enterprise locations or SS7-based networks to disguise the fact that the calls originate

internationally. As noted above, ATIS believes that the governance authority will need to

continually examine how bad actors react to the call authentication frameworks to determine if

changes are necessary to address these evolving threats. The governance authority could also

---

[30] *NOI* at ¶40.

provide guidance and best practices that might reduce or alleviate the challenges associated with international calls.

ATIS submits that the Commission has a key role in coordinating with other countries regarding call authentication issues as well as in educating consumers and service providers on the value of call authentication. ATIS maintains that the Commission should encourage other countries to adopt call authentication frameworks that are compatible with the framework envisioned for the U.S. ATIS has informally met with representatives from both Canada (CRTC) and the United Kingdom (OFCOM) to provide an update on the industry's work. During these meetings, there was a strong interest expressed in what the U.S. is doing to address the issue of unwanted robocalls and acknowledgement that this issue is a global one.

K. Privacy

Privacy issues are also addressed in the *NOI*. In particular, the Commission seeks comment on IETF's assessment that the potential privacy risks associated with a service provider sharing information to authenticate an originator's identity are not significantly different from those inherent in non-authenticated forms of IP-based calling.[31] ATIS agrees with this assessment and notes that the implementation of SHAKEN by the industry is not expected to create unique privacy concerns. ATIS further notes that the industry has considered privacy in its development of SHAKEN and some features of SHAKEN may help to address privacy concerns. For example, use of the SHAKEN OrigID allows the originating service provider to identify the customer while preventing third parties from "reverse engineering" the string to identify the specific customer with which it is associated.

---

[31] *NOI* at ¶ 42.

Comment is also sought on the feasibility, availability, and desirability of certain privacy functions, with the Commission noting that IETF suggests that an entity acting as an authentication service could also act as a privacy service by vouching for the authenticity of a call but not passing along any further identifying information and/or eliminating any identifying information from the call at the originating user's request.[32] This type of functionality is already incorporated in service provider networks (e.g., not displaying caller information at the originating user's request) and is not affected by SHAKEN.

L. Costs

Finally, the Commission seeks comments on the costs of implementing and administrating call authentication arrangements as "telecommunications numbering administration arrangements," and on mechanisms to recover those costs.[33]   While ATIS does not take a position regarding what funding mechanism is appropriate for call authentication arrangements, ATIS notes that a stable funding mechanism must be identified and further believes that: (1) the funding mechanism should allow costs to be equitably distributed among all stakeholders; (2) the funding mechanism should be flexible enough to be quickly modified once the industry has greater experience with the implementation of call authentication arrangements to ensure that the funding is sufficient but narrowly tailored to recovering appropriate costs; and (3) funding levels and mechanisms should be reviewed periodically to ensure that they are appropriate.

---

[32] *NOI* at ¶43.
[33] *NOI* at ¶47.

III. CONCLUSION

ATIS appreciates the opportunity to provide its input to the *NOI* and urges the

Commission to consider the recommendations above.

<div style="margin-left: 50%;">

Respectfully submitted,

Thomas Goode
General Counsel
Alliance for Telecommunications Industry
Solutions
1200 G Street, NW
Suite 500
Washington, DC 20005
(202) 628-6380

</div>

August 14, 2017