Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR

NANC Call Authentication Trust Anchor Working Group

Table of Contents

Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR

1 Introduction

Consistently, Caller ID spoofing and robocalling generate the largest number of consumer complaints to the Federal Communication Commission (FCC), with an estimated 2.4 billion robocalls received by Americans per month in 2016 alone. Recognizing this fact, on July 14, 2017, the FCC issued a Notice of Inquiry seeking comment on the FCC's role in promoting SHAKEN/STIR—an industry-developed set of protocols and operational procedures designed to authenticate telephone calls and mitigate spoofing and illegal robocalling.[1] As part of this administrative process, the FCC has directed the Call Authentication Trust Anchor Working Group (CATA WG) of the North American Numbering Council (NANC) to investigate a variety of issues associated with the SHAKEN/STIR system.[2] Specifically, the FCC directed the NANC CATA WG to address the following substantive issues:

- Define criteria by which a GA should be selected;

- Describe the evaluation process of applying the above-defined criteria;

- Recommend, if the Commission is not to serve as the GA, the role that the Commission should play in overseeing the administration of the call authentication system; and

- Recommend the process by which the PA should be selected, including whether solely by the GA, or by a process including other stakeholders.[3]

Additionally, the FCC directed the NANC CATA WG to address the following procedural steps:

- A reasonable timeline or set of milestones for adoption and deployment of a SHAKEN/STIR call authentication system, including metrics by which the industry's progress can be measured;

- Incentives or mandates that the Commission can put in place to ensure that these milestones and timelines are met;

- Any additional steps the Commission needs to take to facilitate deployment of a call authentication system; and

---

[1] *Call Authentication Trust Anchor,* Notice of Inquiry, 32 FCC Rcd 5988 (2017).

[2] *CATA: Selection of Governance Authority and Timely Deployment,* Letter from FCC Wireline Competition Bureau to Chairman Kavulla of the NANC (Feb. 22, 2018) (Revising a prior Dec. 7, 2017 letter, by extending the deadline to submit a final report to May 7, 2018, from the earlier April 7, 2018, date, and importantly amended the second bullet point which previously directed the CATA WG to "Apply the [GA] criteria in evaluating the suitability of any entities proposing to serve as GA, including ATIS, the Commission, or a working group of the NANC;").

[3] *Id.*

- Any steps the Commission or industry might take to make sure a call authentication system works for all participants in the North American Numbering Plan.[4]

This report summarizes the results of the CATA WG's deliberations and presents additional areas of inquiry which the NANC or FCC should investigate in implementing an effective mechanism to combat spoofing and illegal robocalling.

2   Executive Summary

SHAKEN/STIR is the industry-developed framework of protocols and operational procedures for providing call authentication services. SHAKEN/STIR is an acronym of two sets of technical specifications: the Secure Telephone Identity Revisited (STIR) protocols defined by the Internet Engineering Task Force (IETF)[5]; and the Signature-based Handling of Asserted information using toKENs (SHAKEN) specifications defined by the ATIS/SIP Forum IP-NNI Task Force.[6] Essentially, the SHAKEN procedures utilize STIR protocols to allow communications service providers to attest the legitimacy of a calling party's number. This attestation reflects the extent to which the originating service provider can confirm that the calling party is legitimately entitled to use its indicated phone number. This attestation—included within a Personal ASSertion Token (PASSporT)[7] —is cryptographically "signed" with a "trusted" Secure Telephone Identity (STI) certificate[8] in a manner that allows the terminating service provider to verify the calling party number information. Importantly, SHAKEN/STIR provides the foundation for the development of a real-time authentication of a telephone number which can prevent illegal spoofing and robocalling by identifying any number that cannot be sufficiently attested.

Because the fundamental technologies of SHAKEN/STIR are developed around these STI certificates, the primary goal for a Call Authentication Trust Anchor is to ensure the integrity of the issuance, management, security and use of STI certificates.

To maintain this integrity, SHAKEN/STIR includes three discrete actors: a Governance Authority (STI-GA) which establishes policies for the SHAKEN certificate management framework; a Policy Administrator (STI-PA) which is the day-to-day administrator and primary trust anchor of the system that ensures that STI certificates used to authenticate and verify PASSporT tokens are only available to authorized participants; and Certification Authorities (STI-CA), which issue valid STI certificates.

---

[4] *Id.*

[5] *See generally* [RFC8224], [RFC8225], [RFC8226].

[6] *See generally* [ATIS-1000074], [ATIS-1000080].

[7] *See generally* [RFC8225].

[8] The STI Certifications are based on X.509-based public key infrastructure (PKI) and cryptography. *See generally* [ATIS-1000080].

This report outlines the functional elements, selection process, and characteristics of the STI-GA and the STI-PA, in addition to recommending various milestones, metrics, and incentives to ensure robust participation in the system. This report does not address STI-CAs, nor their role within the SHAKEN ecosystem.

Although SHAKEN provides a mechanism for call authentication, this system does not establish call validation treatment applications (e.g., call blocking or certified identity). This is the next logical step of the Call Authentication ecosystem; however, this is beyond the scope of defining both the STI-GA and STI-PA certificate management functions as part of SHAKEN, and outside the scope of the NANC CATA WG. It is anticipated that these applications will extend the greater STI ecosystem with either enhanced service provider services, or third-party applications offered as enhancements to traditional telephone services.

3 Governance Authority for the SHAKEN Certificate Framework

In the SHAKEN certificate management framework, the role of the STI-GA is to govern the policies and the security around issuance and use of STI certificates by SHAKEN participants in the North American Numbering Plan (NANP).[9] This section discusses the functional elements, legal structure, selection process, and characteristics of the STI-GA.

3.1 Functional Elements of the Governance Authority

The STI-GA should allow for non-discriminatory representation, in the form of a board, by representatives from the communications service provider constituencies. Members should have the requisite expertise to monitor and maintain the certificate and PKI requirements for the ongoing health and security of the SHAKEN certificate management framework. The STI-GA should coordinate with the FCC to ensure transparency in the operation of the ecosystem, as well as cooperate with the FCC on any enforcement actions related to misappropriation of the ecosystem. It should also include functional elements that ensure and support the general day-to-day administration, communications, compliance, privacy and legal functions for both the STI-GA organization, as well as the participants. Finally, there must be ready access to technical expertise that can assist in the policy decisions that impact the SHAKEN certificate management framework, the STI-PA, or the STI-CAs.

---

[9] For the U.S. and its territories, the North American Numbering Plan Administrator (NANPA) is responsible for neutral administration of NANP numbering resources, and its responsibilities are defined in FCC rules and technical requirements approved by the FCC. Operating Company Numbers (OCNs), issued by the National Exchange Carrier Association (NECA), are used to uniquely identify NANP participants per [ATIS-0300251].

To meet these goals, the STI-GA should have three specific functional elements: (i) decision making (comprised of industry representatives); (ii) support (administrative and legal); and (iii) technical (advisory council). The following describes, and provides various guidance, about each of these functional elements.

First, the decision-making element comprised of industry representatives should be the policy and decision-making body of the STI-GA. It should include broad, multi-stakeholder voluntary representation from the U.S. communications service provider sector. The size of the STI-GA should be reasonable to accommodate adequate broad representation, but not too large to hamper an efficient decision-making process. The board must be flexible enough so that it can easily adapt to act quickly to account for new threats and new tactics by bad actors. The suggested target size would be 10-15 board representatives.

Second, the support element comprised of administrative and legal assistance would follow a two-phase process. The development phase would include the required legal and/or accounting resources to establish the STI-GA's legal and business structure. In addition, a small administrative staff of 2-3 personnel would likely be required to handle coordination and communications between stakeholders, as well as holding initial meetings for the STI-PA establishment and selection process. Once the development phase is complete, and there is more limited need for significant support, the administrative overhead should be reduced to operational support as needed, perhaps to periodic or part-time roles and on-demand outside legal and accounting services.

Third, the technical advisory council should be comprised of a three-member council of voluntary experts, which could include board members, that would assist the STI-GA on technical matters. Importantly, this technical advisory council would also serve a liaison role to other technical work relevant to SHAKEN, such as is occurring within the ATIS/SIP Forum IP-NNI Joint Task Force and other relevant standards organizations.

Importantly, these functional elements would allow the STI-GA to provide the following services: (i) administrative; (ii) industry communications and education; (iii) compliance; (iv) privacy and legal support; and (v) technical support.

3.2   Selection of a Governance Authority

The STI-GA selection process is the first step towards formally initiating the organization and setup of the STI and SHAKEN/STIR framework in the U.S. The following describes the selection process for the STI-GA, Board Members, and Technical Advisory Council.

3.2.1   STI-GA Selection Process

To manage the above-mentioned functional roles, we recommend that the industry collaboratively develop a proposal to form an STI-GA. This process has been used successfully for other industry

initiatives, and it allows the industry to begin work immediately without the need for formal FCC comment and rulemaking processes.[10] Additionally, this would allow SHAKEN/STIR to retain maximum flexibility to rapidly respond to evolving threats.

Funding details are outside the scope of the CATA WG report. Yet there are a number of possible funding models, and funding models might be different in start-up mode as opposed to mature operation. For example, founding providers could be required to subsidize certain start-up costs, but funding could evolve over time to make the model self-sustaining (e.g., through certificate fees or licensing fees). However, there is agreement that any funding model should minimize cost barriers to broad representation on a governance board (e.g., representation from multiple service provider constituencies, including small service providers).

3.2.2   STI-GA Board Selection Process

Once a legal entity for the STI-GA has been established, STI-GA board members would need to be selected. Similar to establishing an STI-GA, board member nominees should be selected by the industry. Board member nominees should be vetted for their knowledge and experience relevant to the industry, legal, and technical issues related to SHAKEN framework. For the initial set of STI-GA board members, the nominated individuals could consist of representatives from the following constituencies:

- One large cable provider (perhaps nominated by NCTA);
- One small cable provider (perhaps nominated by ACA);
- One large ILEC (perhaps nominated by USTA);
- One small ILEC (perhaps nominated by NTCA);
- One large wireless provider (perhaps nominated by CTIA);
- One small wireless provider (perhaps nominated by CCA);
- One CLEC (perhaps nominated by INCOMPAS);
- One Regional CLEC (perhaps nominated by a consortium of Western States CLEC Coalition, TEXALTEL and others);
- One OTT VoIP provider (perhaps nominated by VON)

Additionally, for the initial board, there could be board seats available with incentives attached for "founding" members that are early participants in the SHAKEN framework including both technical participation, as well as perhaps financial participation in the initial setup of the STI-GA.

The bylaws of the STI-GA and the ongoing nomination process of the board should be established by the initial board. A suggested board membership term is three (3) years, and terms should be

---

[10] See Appendix § 9.2, noting various industry-developed models where a free-standing legal entity, wholly operated subsidiary, or affiliate of an existing entity are utilized to further various regulatory agendas.

staggered to avoid the loss of institutional memory, and to provide continuity of management. A board member whose term is complete should be eligible for re-nomination for additional terms. If a board member declines re-nomination, resigns, or otherwise needs to be replaced, the board should request new nominees either from the constituency that the member represented, or from the remaining board and industry service provider constituencies. Nominees should be evaluated by the board and selected by majority vote.

While the board will be limited to communications service providers, GA representatives should provide updates, for example, to the FCC's Consumer Advisory Committee's Robocall Working Group regarding relevant consumer issues related to the work of the STI-GA.

3.2.3   STI-GA Technical Advisory Council Selection Process

The selection of the three-member technical advisory council should also involve a nomination process. The STI-GA board should nominate recognized subject matter experts in SHAKEN/STIR standards, certificate management/PKI and communications service provider SIP/IMS deployment. The term of each individual should be three (3) years and terms should be staggered to provide continuity of knowledge and process. Each individual should be eligible for re-nomination at the end of their term. If a technical advisory council member declines re-nomination, resigns, or otherwise needs to be replaced, the board should ask for new nominees. After establishing the initial council, future nominees should be evaluated by the council and selected by majority vote of the STI-GA board.

3.3   Characteristics of a Governance Authority

Once the STI-GA organizational role is established, there are a set of responsibilities and characteristics that the STI-GA must embody. While the original charge of the CATA WG included defining criteria by which a Governance Authority should be selected, it became evident to the group that the STI-GA must be capable of performing specific functions and must have certain characteristics once established. The STI-GA should be established with these characteristics in mind, rather than have these characteristics drive selection. Among the key characteristics were: (i) ability to adapt to change; (ii) openness, neutrality and transparency; (iii) consideration of costs; (iv) accountability; and (v) legal protections. A more detailed list of these characteristics, separated into subcategories, is as follows:

Adapting to Changes

- Flexibility to address evolving threats in a rapid manner;
- Ability to react quickly to integrity issues in the certificate management infrastructure and modify rules, practices, or technology;

- Ability to adapt to changes in legitimate calling practices to avoid false positives, specifically as it relates to changes to STI certificate management that may be required as a result of changing calling practices or the identification of false positives;

- Adaptability to facilitate the enabling of new applications (e.g., analytics for display or blocking), as it relates to changes in STI certificate management and the needs of new applications;

- Ability to manage governance role as use of the Trust Anchor scales;

- Access to industry technical expertise for analysis of issues and trouble-shooting, and open to their input (e.g., IP-NNI Task Force, IETF, 3GPP);

- Ability to evaluate the network impact of proposed modifications to the infrastructure.

STI-GA Participation Model

- Allow for broad/multi-stakeholder participation from service provider constituencies (i.e., technology and size), allowing for direct participation;

- A resilient framework for openness, neutrality and transparency, including consensus-based procedures to define policies to be applied by the STI-PA, in governing STI-CAs and management of the associated PKI;

- A reasonable cost recovery and membership model that allows broad participation without undue cost burdens;

- Sensitivity to maintaining non-discriminatory, competitive and innovative options for SHAKEN call authentication.

Organization/Setup/Processes/Experience

- Minimize cost to the industry so that the STI-GA can fairly allocate costs equitably among all stakeholders;

- Ability to manage expenses and meet budget commitments;

- Ability to manage large, complex projects;

- Ability to manage schedules, milestones and deliverables;

- Ability to get up and running quickly to facilitate legal establishment and board and technical advisory council activities;

- Framework and ability to transition its role to a successor entity if necessary;

- Ability to obtain liability protections or otherwise protect organization and/or members against litigation (e.g., insurable);

- Ability to mediate and resolve disputes;

- Ability to understand and incorporate end user constituency concerns;

- Capable of working in a "hybrid" structure with the FCC;

- Ability to define governance model and STI-GA board decision-making/voting processes;

- Auditable finances;

- Ability to enter into a contractual relationship with/contract for a STI-PA;

- Mechanisms to charter technical expertise (e.g., working groups) and operate a standardization-like process.

3.4   Role of the FCC

In the event the FCC supports an industry-led entity to govern the SHAKEN/STIR ecosystem, the FCC would not serve as the STI-GA, and the FCC would not need to formally authorize the model recommended for forming an STI-GA. This would allow its start-up to be expedited and streamlined. There are nevertheless significant roles which the FCC could assume.

The FCC should serve in an oversight role that includes driving progress toward industry call authentication objectives and timelines. However, FCC action may ultimately be necessary to address the issues raised in Sections 5.2 and 5.3 of this report. In addition, the FCC could ideally act as an escalation point for resolution of grievances that have come before the STI-GA, but remain unresolved after an STI-GA decision. The STI-GA should provide a progress report at each NANC meeting, including milestones in testing and implementation of SHAKEN/STIR. It is expected that the STI-GA would remain accountable to the FCC in terms of reporting to the NANC. Finally, the FCC could play a significant role in establishing incentives for service providers to participate in SHAKEN/STIR, as further described in this document.

4   Policy Administrator for the SHAKEN Certificate Framework

The STI-PA in the SHAKEN framework administers the technical operations and execution of the policies and verification of participants that are authorized to participate in the SHAKEN ecosystem. The STI-PA will apply both the policy and direction of the STI-GA consensus, as well as conform to the technical specification of the SHAKEN certificate framework, as they evolve to ensure security and integrity in the SHAKEN ecosystem.

4.1   Functional Elements of the Policy Administrator

The STI-PA roles are defined in the SHAKEN certificate management framework, and the Certificate Management and Operational Considerations for the STI-CA and STI-PA.[11] These roles include the following:

- Approval of SHAKEN compliant STI-CAs and certification of their operation in compliance with certificate practices;[12]

---

[11] *See generally* [ATIS-1000080], [IPNNI-2018-0004RXXX].
[12] *See generally* [IPNNI-2018-0004RXXX].

- Confirmation and authorization of service providers and their associated information that represents their authorization and their associated telephone numbers uniquely in STI certificates;

- Issuance and periodic renewal of Service Provider Code (SPC) tokens to authorized service providers;

- Maintenance and distribution of the up-to-date list of valid root certificates corresponding to approved STI-CAs;

The STI-PA, like the STI-GA, should have two phases of general operation. The first phase should be the start-up and organizational phase. This phase would include these main components:

- Management portal for accessing STI-PA services including account registration and selection of preferred STI-CA(s);

- Development of SHAKEN certificate management framework defined API for service provider acquisition of SPC token(s);

- Development of the API for getting the current list of approved STI-CAs;[13]

- Operational organization of managing and securing services to support the above software, as well as organizing the verification of service provider credentials when seeking to acquire certificates and ownership of SPCs when establishing an account with the STI-PA.

As an ongoing operational role, the STI-PA should perform the following:

- Management and maintenance of uptime and availability of the services and support for its customers for the STI-PA API services through a small operational team (1-2 personnel);

- Periodic contract software maintenance for implementing any new technical requirements that may come from STI-GA decisions or industry standards updates;

- Periodic reporting and metrics back to the STI-GA;

- Issue tracking, reporting of potential service provider, STI-CA, or bad actor errors, not following best practices or fraudulent activities.

4.2   Selection of a Policy Administrator

The STI-PA should be selected through a Request for Proposal (RFP) process, or other transparent process initiated by and overseen by the STI-GA Board. The RFP or selection criteria should include specific requirements based on the above noted functional elements, ensuring that a selected STI-PA has the necessary track record, experience, management, security and operational capabilities to perform this role and the ability to commence effective operations within the required time frame. There should be, at a minimum, an appropriate legal or financial separation between the STI-GA and an organization being considered for the STI-PA to avoid any potential conflicts of interest. The STI-PA should be selected in a manner that minimizes cost to the industry and disruption to SHAKEN as

---

[13] *See generally* [IPNNI-2018-0004RXXX].

it evolves. The WG recommends that the contract should be terminable at will and be non-exclusive. Additionally, a contract must accommodate flexibility to allow for changes as the SHAKEN model may evolve. STI-PA contracts could be re-bid if deemed necessary by the STI-GA.

An STI-PA contract should be subject to review at any time if they fail to meet the obligations established by the STI-GA or compliance with the SHAKEN specifications, with a process spelled out in the STI-GA bylaws. The STI-GA bylaws should detail all conditions that the STI-PA contract should be subject to review.

Additional consideration on this subject are summarized as follows:

Process

- The Governance Authority for SHAKEN/STIR should provide a framework for the authorization, certification and governance of an STI-PA.
- The STI-GA should drive an RFP or other transparent process to select the most suitable STI-PA.
- Any RFP or other transparent process should be under the direct oversight of the STI-GA Board.
- The STI-GA Board, consisting of representative stakeholders from wireless, incumbent wireline, competitive wireline, VoIP and rural sectors, should develop an RFP or identify another transparent process to select the STI-PA.
- An RFP or other transparent process should focus on attributes regarding track record, experience, management, security and operational capabilities.
- The STI-GA should lead the process with FCC support to maintain the industry leadership on the trust anchor framework. The industry-led structure offers flexibility to adapt to evolving threats without having to go through a rulemaking or other formal regulatory process.
- An STI-GA must be neutral and have no conflicts of interest such as common ownership or management with any STI-PA candidate that it evaluates.

Participation Model

- Governance of an STI-PA should be managed and monitored by the STI-GA to a set of criteria that allows the sharing of the authorized STI-CA information.

Other Factors

- An STI-PA should be selected in a manner that minimizes cost to the industry and disruption to SHAKEN as the ecosystem evolves.
- The selection process for an STI-PA should leverage ongoing industry work by bodies such as the ATIS/SIP Forum IP-NNI Task Force.

5 Deployment of the SHAKEN Certificate Framework

The goal of the CATA WG—beyond recommending the process for establishing the structural components necessary to maintain and secure the SHAKEN framework, and hastening its general deployment and operations—is to encourage swift participation in the ecosystem by communications service providers, vendors, and other legitimate participants. The WG recommendations support the strategic goal of enabling secure and trustworthy validation of calling identity for telephone calls. Achieving the goal, however, requires a coordinated effort by the FCC, communications service providers, and others in the ecosystem. The following section includes recommendations for measuring deployment progress, incentivizing participation, and addressing additional concerns.

5.1 Milestones

The CATA WG recommends the target timeline, as set forth below, for establishing a governance structure for the Trust Anchor. Any prospective changes to these timelines would be reported to the NANC. It should also be recognized, however, that establishing the governance structure is not a mandatory prerequisite to deploying the SHAKEN/STIR framework. Service provider interoperation may occur in parallel with the STI-GA establishment and STI-PA selection processes. This will allow for implementation of the framework among peers pursuant to a more aggressive timeline.

- The STI-GA should be established within no more than three months after the NANC submits its report to the FCC.

- The STI-GA should issue an RFP or initiate an alternate transparent process for selection no more than three months after establishment.

- The submission of the RFP responses or alternate transparent process should not exceed a period of three months.

- The STI-GA should select an STI-PA no more than three months after conclusion of an RFP response deadline or three months after the initiation of an alternate transparent process for selection of an STI-PA.

- We encourage the participants in the above activities to expedite any steps and shorten timelines where possible.

In general, the WG agrees that it is important for the FCC to have timely information that provides adequate detail regarding industry progress toward implementation of the framework. In furtherance of that objective, the WG recommends that the STI-GA provide to the NANC a progress report on the implementation of the framework for presentation at each NANC meeting. The progress report could include: (i) quantitative information (e.g., the number of providers participating in a testbed or the live platform when deployed, transaction detail record summaries, the number of signed calls over the last quarter, etc.); and (ii) qualitative information on milestones for implementation of SHAKEN (e.g., formation of the STI-GA board, release of an RFP for the STI-PA, successful

validation of the framework, methods or recommendations for funding the ecosystem, etc.). If progress were deemed by the Commission to be lagging beyond reasonable expectations it could direct service providers to start actively testing in either direct interoperability tests or as part of coordinated industry testing.

5.2   Incentivized Participation

In terms of incentives for participation in the SHAKEN ecosystem, the WG recommends that the Commission provide some level of liability protection for communications service providers who take reasonable steps to identify the level of trust associated with calls that utilize the SHAKEN framework.

For example, a safe harbor for unintended blocking or mis-identification of the level of trust for individual calls would provide a strong incentive for communications service provider adoption of SHAKEN, particularly where analytics are overlaid on the framework. Such liability protection may override reluctance to participate in SHAKEN, particularly in its early stages. The FCC can also speed or promote more widespread adoption by incentivizing IP-to-IP interconnection for voice service providers because of the IP-to-IP connectivity required for the most fulsome level of attestation that can occur under the SHAKEN framework. Encouraging adoption of a governance model that minimizes cost to the industry, and relatedly to consumers, is also important for incentivizing widespread adoption of the framework.

Additionally, to ensure that SHAKEN works for the broadest array of NANP participants, the FCC should encourage development of a funding structure that allows for broad service provider participation on the STI-GA board, which may be achieved through adequate funding for establishing the STI-PA. Depending on the ultimate governance structure endorsed by the Commission, and any requisite legal authority, the FCC might consider whether the STI-PA (which could entail the most extensive start-up costs), and possibly the STI-GA, be funded through the NANP (either initially or ideally on an ongoing basis). The Commission could also ensure that a sufficient escalation path exists for resolving disputes or deficiencies in the SHAKEN framework. More specifically, if a framework participant registers a grievance against the STI-PA or an STI-CA, an escalation path, after exhausting potential remedies through the STI-GA, should include an option to escalate to the Commission or an FCC advisory committee such as the NANC.

5.3   Additional Concerns

In implementing a Call Authentication system, the FCC and involved parties should ensure that certain additional threshold issues are addressed.

First, as SHAKEN is deployed across communications service providers and begins to mitigate illegitimate caller ID spoofing and illegal robocalls, bad actors will modify their behavior to work around the system. As spam call detection services put basic measures in place, for example to

identify invalid numbers or unallocated numbers (e.g., 000-000-0000), illegal robocallers are increasingly falling back to spoofing valid numbers. For example, robocallers spoof numbers from the target customer's local calling area (i.e., neighbor spoofing). This makes it harder to distinguish legitimate calls from illegitimate calls, both for the consumer and the spam call detection services, which ultimately undermines the system. Relatedly, once SHAKEN becomes implemented across a large percentage of calls, callers making illegal robocalls will find and exploit vulnerabilities in the SHAKEN and certificate management framework. As a result, the STI-GA cannot be solely based on today's network context; rather the principles must be structured to adapt to this dynamic environment.

Second, the STI-GA must recognize that SHAKEN/STIR provides an enabling infrastructure. The STI-PA, on behalf of the STI-GA, focuses on ensuring the integrity of that enabling infrastructure, and in particular the management and proper authorization of STI certificates. The many possible applications that will take advantage of the call authentication provided by SHAKEN/STIR are outside scope for the STI-GA and the CATA WG. However, the STI-GA must be structured to enable these applications to operate in the ecosystem, subject to enforceable, but neutral and transparent policies.

In general, it should also be recognized that service provider interoperation, vendor implementation and deployment of the SHAKEN/STIR framework should continue in parallel with the STI-GA establishment and STI-PA selection processes. This will ensure as much parallel effort as possible for coming together from both sides of the VoIP network deployment and the certificate management infrastructure and authorization mechanisms to secure the certificates with a common Trust Anchor.

6 Update on Deployment of the SHAKEN SIP Framework

As detailed in the Robocall Strike Force Report and continued in the Robocall Strike Force Report update, SHAKEN/STIR and specifically the SHAKEN SIP Framework are a key component of the overall system to both protect consumers against illegal robocalls by carrying the cryptographic signatures and providing secure information for reliably and efficiently tracing back identified illegal calls to the communications service providers that can identify the origin, e.g., to facilitate enforcement actions by FTC or FCC. In order to achieve these goals with SHAKEN/STIR, of key importance, is the signing of all or almost all domestic legitimate calls. This was also noted in the December 7, 2017 letter from Kris Monteith to the NANC: "For call authentication to effectively and reliably authenticate calls, a substantial majority of calls – and thus significant number of providers – will need to participate in the system."

Once this is achieved, many unsigned domestic calls have a high probability to be unwanted, and thus providing an indication of validated identity or for non-validated calls a warning of the identity has not been validated, consumers or communications service providers, acting on their behalf, may summarily reject such calls. Because spoofing allows rapid change of numbers by bad actors, existing

mechanisms like blacklists while somewhat effective, have proven to become less effective due to illegal robocalls starting to use already allocated numbers that may already be used by legitimate telephone subscribers.

The above referenced letter from Kris Monteith to the NANC also calls for a "reasonable timeline or set of milestones for adoption and deployment of a SHAKEN/STIR call authentication system". As the deployment of SHAKEN/STIR grows, once we achieve a point where a large percentage of communications service providers sign calls, any remaining communications service providers that are not signing their calls should be well incentivized to also sign their call since they would otherwise risk that many of their customers' calls will be rejected, putting that provider at a distinct competitive disadvantage. As a provider of telephone service to consumers, there should be incentives to sign calls for better answer seizure ratios (ASR) providing more consumer satisfaction and more consumer trust in the telephone service. A specific voluntary industry-wide timeline for implementation of SHAKEN/STIR into the communications service provider network and correspondingly to the diverse set of VoIP equipment and software vendors would be a way to move those providers and vendors that haven't already showed progress towards this goal, as discussed in the Robocall Strike Force report in October 2016 and update in April 2017, to implement SHAKEN/STIR. Such an agreement is likely to focus implementation efforts. It is interesting to note, that in Canada the CRTC has stated that it "expects" implementation of SHAKEN/STIR for all VoIP calls by March 31, 2019[14] which will also incentivize many of the equipment vendors to implement these features in their software to serve their Canadian customers.

While there is already progress with many providers shown in the Robocall Strike Force update, it is quite likely that getting to a large percentage of calls with SHAKEN/STIR call authentication will only occur, and fulfill the promise of SHAKEN/STIR if there is a formal commitment of service providers to implement the framework by a particular target date.

Concerns have been expressed that small communications service providers will not be able to handle the additional responsibility of implementing SHAKEN/STIR based on equipment or economic concerns. However, small carriers may already utilize third party service providers to gateway long-distance calls, including VoIP calls, and thus may be able to delegate the responsibility to those large entities. It should be acknowledged that unwanted robocalls may originate on VoIP-to-TDM gateways from domestic carriers. Nonetheless, to the extent implementation of SHAKEN/STIR is mandated by regulatory directive, the Commission must consider potential means of cost recovery for such implementation, particularly for smaller providers, other than through increased end user rates that may render such rates unaffordable. This is necessary because it is not in fact the case that most or all small carriers utilize third party service providers to gateway long-distance calls, and thus some small carriers may be unable to delegate the responsibility to those large entities (or, at the very least,

---

[14] See Canadian Radio-Television and Telecommunications Commission, *Compliance and Enforcement and Telecom Decision CRTC 2018-32,* January 2018.

to do so without significant increased cost). As a complementary measure, the Commission should establish a categorical exemption for small providers that do not originate VoIP calls, which would be consistent with the Canadian focus only on VoIP calls.

Thus, we recommend two steps that will accelerate deployment:

1. Ensure that all carriers that route calls between originating and terminating carriers, such as long-distance providers and least-cost routers, maintain the integrity of the required SHAKEN/STIR signaling.

2. Second, given the varying degree of technological capabilities between communications service providers, as well as the nascent stage of vendor products capable of supporting SHAKEN/STIR, it will not be technologically feasible to implement the standard in a uniform timeframe throughout the industry. However, individual companies capable of signing and validating VoIP calls using SHAKEN/STIR should implement the standard within a period of approximately one year after completion of the NANC CATA report. This pragmatic approach ensures that companies capable of deploying the standard will be encouraged to do so, while also acknowledging the technical realities of deploying the standard throughout all categories of providers. Such an approach also avoids setting unrealistic expectations for consumers and all stakeholders.

Mandates should be unnecessary as service providers voluntarily implement SHAKEN/STIR consistent with technologically pragmatic timelines such as the one recommended above. As SHAKEN/STIR is deployed by providers, the evolving nature of the technology and the growing levels of deployment will enhance the ability of industry stakeholders in multiple areas. Even in the early stages of deployments, these enhancements will include increased ability to trace illegal robocalls, improved call analytics for consumer tools, and more effective enforcement actions. Reporting on the percentage of IP voice calls using SHAKEN/STIR would also provide the necessary accountability to encourage timely deployment.

7 Steps to be Taken to Make Sure Call Authentication Works for All Participants in the NANP

The SHAKEN/STIR framework will not "solve" illegal caller ID spoofing, but it is an enabler that can lay the groundwork for a variety of techniques to address the problem as enumerated in this report and previous Strike Force reports. This includes the end-to-end authentication of the telephone number as well as a reliable and efficient method for doing trace back on calls that are found to be illegal, if a perpetrator is bold enough to sign their illegal call as a legitimate verified call. Similarly, establishing the Call Authentication Trust Anchor (STI-GA/STI-PA) will not by itself ensure that the call authentication system works for all participants in the North American Numbering Plan. Consistent with the recommendations of this report, the establishment of a secure certificate management infrastructure for SHAKEN (the primary objective of the STI-GA and STI PA) will provide the necessary building block for securing the call authentication behind the legitimate participants in the North American Numbering Plan.

8 Conclusion

This report contains recommendations of the NANC CATA WG for the efficient, secure, expeditious, cost effective, industry-led establishment of the STI-GA and subsequent STI-PA functional elements of the SHAKEN/STIR framework. The primary focus is the establishment of the STI-GA and the industry and technical representation in that organization. Guidance for the selection and establishment of the STI-PA is also provided. Further, a set of milestones, metrics, incentives, and participation guidance that defines both industry and regulatory roles in achieving the efficient, legal framework for the successful deployment of SHAKEN/STIR are provided. Ultimately, our goal as participants in the communications industry, whether as providers of end user services, vendors of systems and equipment, regulators, and as consumers ourselves, is the protection of consumers from the fraud, annoyance, and other ills that result from unwanted and illegal robocalls. Implementation of the SHAKEN/STIR framework is an efficient and prudent way to ensure the security and protection of the telephone ecosystem.

The completion of technical work and guidance of the ATIS/SIP Forum IP-NNI Task Force and IETF representing the SHAKEN and STIR combination of technical specifications and the drive of the FCC Robocall Strike Force represented the first phase of this deployment. The NANC CATA WG recommendations in this document, focused on establishing legal entities that will represent the SHAKEN framework in the U.S., are a critical second phase that will bring us to the point of establishing the end-to-end framework for telephone calls and the security around the authentication and verification of calling identities. We respectfully submit this report as a plan of action to achieve the above goals and move forward as an industry to successfully protect our treasured resource of the national communications network.

9 Glossary

FCC – Federal Communications Commission. The FCC may also be referred to in this document as "the Commission."

NANP – the North American Numbering Plan is the basic numbering scheme permitting interoperable telecommunications services within the U.S., Canada, Bermuda, and most of the Caribbean.

PASSporT – the core token used to transmit the signed information corresponding to the Caller ID of the caller and the call itself, as defined in [RFC8225]

SHAKEN framework – both the SIP protocol framework defined in ATIS-10000074 that uses IETF STIR protocols defined in RFC8224 and RFC8225 to form an industry framework for the deployment of STI in service provider networks and the certificate management framework defined in ATIS-1000080 that uses IETF STIR defined certificates in RFC8226. It may also be referred to in this document as "the framework."

SPC – a generic term for the identifiers used to designate service providers in telephone networks today. In North American context, these would include OCNs as specified in [ATIS-0300251], related SPIDs, or other similar identifiers for service providers. SPCs can be used to indirectly identify all of the telephone numbers associated with a service provider.

STI – Secure Telephone Identity, used to refer to the overall idea of securing the Caller ID or telephone number.

STIR – The IETF working group Secure Telephone Identity Revisited where the core protocols used for SHAKEN are defined, RFC 8224, RFC 8225, and RFC 8226.

10 References

ATIS-1000074, Signature-based Handling of Asserted Information using Tokens (SHAKEN), *https://www.atis.org/docstore/product.aspx?id=28297*.

ATIS-1000080, Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management, *https://www.atis.org/docstore/product.aspx?id=28345*.

- NOTE: ATIS-1000074 and ATIS-1000080 are available on the SIP Forum website to those without ATIS access

ATIS-0300251, Codes for Identification of Service Providers for Information Exchange, *https://www.atis.org/docstore/product.aspx?id=26148*.

IPNNI-2018-0004RXXX, Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators, *http://access.atis.org/apps/group_public/document.php?document_id=39158&wg_abbrev=ipnni*.

- NOTE: All IP-NNI documents are publicly available

RFC8224, Authenticated Identity Management in the Session Initiation Protocol, *https://tools.ietf.org/html/rfc8224*.

RFC8225, Personal Assertion Token (PASSporT), *https://tools.ietf.org/html/rfc8225*.

RFC8226, Secure Telephone Identity Credentials: Certificates, *https://tools.ietf.org/html/rfc8226*.

11 Appendix

11.1 Future Considerations for Governance or Technology Advisory to Technology Standards

There were a limited number of issues or recommendations raised in the CATA WG determined to be out of scope for our referral charge. The CATA WG did, however, acknowledge the importance of addressing the issues or recommendations, some of which would be more appropriately tackled by technical bodies. A description of the considerations (some of which are already being addressed by technical bodies) are as follows:

- The Commission should continue to encourage the development of a call authentication framework across multiple communications signaling platforms. Many voice calls are still transported over TDM networks and ubiquitous deployment of IP networks, particularly in rural areas, is many years away. As a result, the application of SHAKEN/STIR in non-SIP environments should not be ignored. The work at the IETF STIR Working Group on an out-of-band STI architecture offers one potential solution.

- Pursuant to an RFP or other transparent selection process, an initial STI-PA should be selected per ATIS Standard (ATIS-1000080). Consideration of the potential use of multiple STI-PAs should be evaluated by the IP-NNI Task Force for technical and security considerations and potential inclusion into the SHAKEN specifications.

- STI-GA experience should include the ability to establish privacy and security protections – i.e., to secure data and protect against breaches (PII and CPNI).

- An STI-PA must be neutral and have no conflicts of interest such as common ownership or management with any STI-CA candidate that it evaluates.

11.2 Industry Examples of Models for STI-GA Legal Entities

There are a number of industry models that could be used to establish an industry-deployed and industry-led STI-GA, including initiatives in the communications sector where an independently

organized governance structure was established. A combination of the best characteristics of these models could be used to create the STI-GA. Models considered included:

DFAST: Under DFAST (manufacturer licensing for use of CableCARD), the Governance Authority established license terms, including authorization to receive X.509 security certifications. The STI-GA entity could similarly establish a standard agreement, to be signed by each participating service provider, covering the terms for grant, use and revocation of certificates. It could also establish detailed rules to be implemented by the STI-PA.

Energy Voluntary Agreements: Similar to the model for Energy Voluntary Agreements (VAs) for set-top boxes and small network equipment, the STI-GA could have a governing board (this is called a Steering Committee under the VAs), comprised of participating communications service providers.

CA/Browser-Forum: The CA/Browser-Forum is an example of an organization that sets technical and operational requirements for X.509 CAs and web browsers.

Administrative Council for Terminal Attachments (ACTA): The FCC's selection of the Administrative Council for Terminal Attachments (www.part68.org) is an example where a multi-stakeholder group—similar to that proposed in this report—was utilized to implement a regulatory agenda, as opposed to a federal regulatory body or federal advisory committee. On May 22, 2000, the FCC released a Notice of Proposed Rulemaking (NPRM) in CC Docket No. 99-126 to seek comment on ways to streamline the process by which technical criteria are established for customer premises equipment that must be allowed to connect to the PSTN. As part of this NPRM, the FCC also proposed to assign to private industry the process of verifying that specific equipment meets the established technical criterial and requested parties to submit their proposals for the manner in which a "gatekeeper SDO" should be structured.

On December 21, 2000, the FCC released its Report and Order (R&O), which required the industry to establish the ACTA and identified the industry sponsors (ATIS and TIA) for this activity. The FCC noted that the selection of these industry multi-stakeholder groups would best serve its goal of ensuring broad-based industry participation in the ACTA's activities and responsibilities. (R&O at ¶43).

The FCC also agreed that the ACTA should be a committee of interested industry experts that will, subject to the FCC's guidelines and procedures, perform the functions of publishing technical criteria proposed by ANSI-accredited SDOs and maintain a database of approved terminal equipment. (R&O at ¶31). The FCC noted that private industry was well equipped to take over all functions except enforcement and final appeal processes. (R&O at ¶32). The FCC further found that "the industry Administrative Council model is the one best able to ensure continuity in the development of technical criteria for terminal equipment while, at the same time, enabling the industry to develop rapidly equipment for the provision of advanced services." (R&O at ¶43).

The FCC considered but ultimately decided against the formation of a Federal Advisory Committee, noting that "[e]stablishing a FAC would not achieve [its] goals of reduced governmental involvement in the standards process and expedited development of technical criteria for new technology." (R&O at ¶35).

Finally, the FCC determined it is not necessary to establish a term limit for the sponsor but did retain oversight of the ACTA to ensure that no anti-competitive or other discriminatory practices hinder the work of the ACTA. (R&O at ¶¶47, 48). The FCC further concluded that it was not necessary for it to establish specific funding mechanisms for the ACTA, finding that the ACTA and the joint sponsoring organizations were in the best position to determine financing arrangements. (R&O at ¶56).

Minority Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR

Henning Schulzrinne

Minority Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR

This minority report provides alternative recommendations to those provided in Sections 3.2.2 ("STI-GA Board Selection Process") to ensure that all relevant and affected stakeholders are included in the governance of its deployment.

The Secure Telephone Identity eco system affects carriers, as implementors, but its goal is to protect consumers against unwanted robocalls. The STI-GA is the only on-going policy-making entity in this space, except for the FCC itself. It will likely determine who gets to sign calls, which entities need to report what kind of information to whom and with what frequency (Section 5.1 of the Report), which CAs get authorized and how soon all the various components are put in place and start to perform their assigned duties. All of these affect the speed, efficacy and efficiency of implementing STIR/SHAKEN and thus the timing of when consumers will experience relief from unwanted robocalls. This is particularly true if the FCC takes a hands-off approach and leaves implementation of STIR/SHAKEN to industry.

In the future, entities other than carriers, such as large enterprises, may want to or need to sign calls, as they may be using multiple VoIP carriers and place, with the permission of the customer currently holding the number, outbound calls on behalf of that customer. For example, outbound call centers and notification and alerting services may use the number of the airline, school district or doctor's office they are placing calls on behalf of. Unfortunately, all of the proposed board members have a potential conflict of interest, as they may prefer to offer such services themselves. *Thus, the STI-GA should include a representative reflecting the interest of large telephony users.*

Consumers are both directly affected and have a stake in the policy decisions of the STI-GA. For example, decisions of the STI-GA will affect how soon STIR/SHAKEN is widely implemented, the type of reporting requires by other entities, such as the STI-PA, STI-CAs and the carriers. (The STI-GA, STI-PA, STI-CAs will have no direct knowledge of the volume of calls signed, for example, and would have to require such reporting by imposing it as an obligations on recipients of certificates.) Longer term, the STI-GA may affect, through its policy requirements, the level of assertions provided, and whether and when non-carrier entities can sign calls. Having consumers represented on the board ensures that they can be heard and participate in decision making. Such participation also adds credibility to an organization that, after all, only exists to protect consumers. The state utility commissions serve, inter alias, to protect the interests of consumers in their jurisdictions.

There are several possible organizations that could nominate such board members. I propose to have two non-carrier board members: one board member nominated by NARUC and one by the consumer group members of the FCC Consumer Advisory Committee or drawn from one of the consumer entities that have been most active in this area (e.g., Consumers Union).

Since there are no technical qualifications to serve on the board (e.g., an engineering degree or evidence of technical knowledge), beyond a general understanding of the functioning of the overall STIR/SHAKEN system, it is likely that the board members nominated by the various industry associations and any consumer organizations are similarly qualified.