



131 NW First Avenue, Delray Beach, Florida USA 33444  
+1-561-232-3891  
[www.cloudcommunications.com](http://www.cloudcommunications.com)  
[jmarion@cloudcommunications.com](mailto:jmarion@cloudcommunications.com)

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

<i>In the Matter of</i>	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

**Comments of the Cloud Communications Alliance**

Joe Marion  
President  
Cloud Communications Alliance  
131 NW 1st Avenue  
Delray Beach, FL, USA 33444  
(561) 232-3891

July 24, 2019

## TABLE OF CONTENTS

	Page
I. INTRODUCTION AND SUMMARY.....	1
II. THE COMMISSION SHOULD NOT ADOPT SAFE HARBORS FOR BLOCKING BASED ON SHAKEN/STIR INFORMATION UNTIL THE FRAMEWORK IS FULLY IMPLEMENTED.....	2
A. Status of SHAKEN/STIR and Open Issues.....	2
B. Critical Aspects Of The Framework Remain Under Unresolved.....	5
III. SAFE HARBORS, IF ADOPTED, SHOULD REQUIRE IMPLEMENTATION OF EFFECTIVE AND TIMELY MECHANISMS TO PROMPTLY ADDRESS INADVERTENT OR ERRONEOUS BLOCKING OR LABELING OF LEGITIMATE CALLS.....	9
IV. INTERNATIONAL CALLS SHOULD NOT AUTOMATICALLY BE BLOCKED.....	11
V. CONCLUSION.....	11

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

<i>In the Matter of</i>	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

**Comments of the Cloud Communications Alliance**

**I. Introduction and Summary**

The Cloud Communications Alliance (“CCA”) hereby submits these comments in response to the Third Further Notice of Proposed Rulemaking in the above captioned proceedings.<sup>1</sup> CCA members are committed to the eradication of unlawful “robocalls” that are disrupting communications networks and costing consumers millions of dollars in fraudulent scams. The SHAKEN/STIR framework is a promising tool to address this problem by enabling originating voice service providers to authenticate their customers’ authority to use the numbers appearing in caller ID. Although laudable, the framework is still undergoing development in many critical respects. Authorizing safe harbors for blocking any calls based on SHAKEN/STIR information is thus premature, particularly if unaccompanied by requirements to promptly and efficiently address erroneously blocked calls.

---

<sup>1</sup> *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, CG Docket No. 17-59, WC Docket No. 17-97, FCC 19-51 (rel. June 7, 2019) (“Declaratory Ruling” or “Further Notice”); Consumer and Governmental Affairs Bureau and Wireline Competition Bureau Announce Comment Dates for Call Blocking and Caller ID Authentication Third Further Notice of Proposed Rulemaking, Public Notice, CG Docket No. 17-59, WC Docket No. 17-97, DA 19-597 (June 26, 2019).

CCA is the leading affiliation group representing the Cloud Communications industry globally. The rapidly growing association represents cloud services providers of unified communications systems for enterprise customers and their vendors. The CCA serves as a “Voice for the Cloud Communications industry” as it represents thought leadership worldwide for financial and industry analysis, regulatory issues, and innovation. CCA members’ solutions enable businesses of all sizes to utilize efficient and sophisticated communications technologies, including voice over internet protocol (“VoIP”) calling platforms, without incurring costly capital expenditures. For the most part, CCA’s members provide over-the-top services that utilize the customer’s broadband connection. Many members also obtain telephone numbers from carrier-partners that may also facilitate interconnection with other IP-providers or the PSTN. CCA members collectively serve more than 20 million “seats.” Seats are a common metric for software licensing and in this context is roughly equivalent to an individual line or station.

## **II. The Commission Should Not Adopt Safe Harbors for Blocking Based on SHAKEN/STIR Information Until the Framework is Fully Implemented**

### **A. Status of SHAKEN/STIR and Open Issues**

The SHAKEN/STIR framework is designed to pass information known by the originating service provider through one or more networks to the terminating provider.<sup>2</sup> The framework contemplates three levels of attestation. The “highest level” or A-level attestation, constitutes a verified assertion by the originating provider that it knows the caller and that the caller is

---

<sup>2</sup> Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR, NANC Call Authentication Trust Anchor Working Group at 4 (“NANC Report”) available at [http://nanc-chair.org/docs/mtg\\_docs/May\\_18\\_Call\\_Authentication\\_Trust\\_Anchor\\_NANC\\_Final\\_Report.pdf](http://nanc-chair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf) (last visited July 23, 2019) (“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.”)

authorized to use the calling number. A B-level attestation asserts that the originating provider knows the calling party, but cannot confirm that the calling party is authorized to use the number. The “lowest” level of attestation, the C-level or gateway attestation, signifies that the signer does not know the customer or the number, it simply knows that the call has entered its network at a specific point. This would typically apply to international calls.

The SHAKEN/STIR framework establishes a mechanism to transmit the attestation in a trusted manner from the originating to the terminating provider, including through intermediate carriers. The framework is currently designed to work with SIP protocols and thus requires end-to-end IP treatment of the call. An equally important aspect of the framework enables tracing the call back to its origin. It contemplates assigning unique numerical identifiers to originating providers or callers that can be used to identify bad actors. Several major carriers have begun to implement the mechanics of signing and transmitting verified calls either within their own network or between select other providers that have implemented aspects of the framework, although this initial implementation appears limited to calls originated by residential customers, not business customers.

The framework also contemplates an industry-led governance structure that develops and implements rules and oversees and dispenses the certificates needed to participate and sign trusted calls. Based on a directive by the Commission, the North American Numbering Council (NANC) made recommendations regarding the governance structure that were approved by Chairman Pai.<sup>3</sup> The governance structure contemplates three discrete roles: A Secure Telephone Identity Governance Authority (STI-GA) that sets policy; a Policy Administrator (STI-PA) that implements those policies and is the primary trust anchor for the framework; and Certification

---

<sup>3</sup> Press Release, Federal Communications Commission, Chairman Pai Welcomes Call Authentication Recommendations From The North American Numbering Council (May 14, 2018) available at <https://www.fcc.gov/document/charman-pai-welcomes-call-authentication-framework> (last visited July 18, 2019).

Authorities (STI-CA) that issue valid STI certificates to qualified participants. Parts of the governance are in place. The Governance Authority has been established and the PA was recently selected.<sup>4</sup> The Certification Authorities have yet to be approved.<sup>5</sup>

Industry is to be lauded for progressing as quickly as it has in implementing this new, complex framework. Yet critical aspects of the framework remain unresolved and under review. Among the issues still to be resolved in a uniform fashion are how the SHAKEN/STIR information will be presented to the called party.<sup>6</sup> Cost recovery also remains an open question and may require Commission involvement and is an important issue for smaller providers. In previous instances where the Commission has established network obligations that benefit consumers at large, such as with number portability, the Commission also developed mechanisms for recovering costs.<sup>7</sup> Industry is still grappling with the implementation of

---

<sup>4</sup> iconectiv was selected as the PA on May 30, 2019. Press Release, iconectiv, Mitigating Illegal Robocalling Advances with Secure Telephone Identity Governance Authority Board's Selection of iconectiv as Policy Administrator (May 30, 2019) available at <https://iconectiv.com/news-events/mitigating-illegal-robocalling-advances-secure-telephone-identity-governance-authority> (last visited July 23, 2019).

<sup>5</sup> Earlier in July, the STI-GA issued a call for parties interested in becoming CAs. It hopes to have the governance apparatus operational by December 11, 2019. See Press Release, iconectiv, STI-GA Call for Certificate Authorities (July 9, 2019) available at <https://iconectiv.com/news-events/sti-ga-call-certificate-authorities> (last visited July 23, 2019).

<sup>6</sup> One display method under consideration is a green checkmark that would signify that the call has been properly authenticated under the SHAKEN/STIR framework. As was recently pointed out, however, because the “intent of calls cannot be attested to and because callers with fraudulent intent will be able to make outbound phone calls from telephone numbers which have legitimately been assigned to them, we suggest it is possible that providing a green checkmark or other verification display runs the risk of conferring validity to the phone call beyond the display’s intent.” Letter from Deirdre Menard, LucidTech LLC, to Marlene H. Dortch, FCC, CG Docket No. 17-59, WC Docket No. 17-97 (filed June 20, 2019). See also Letter from Amanda E. Potter, AT&T, to Marlene H. Dortch, FCC, WC Docket No. 17-97 at 2 (filed November 19, 2018) (noting timing and format for consumer displays remain under discussion and that proper displays are “critical to ensure that service providers do not inadvertently miscommunicate the meaning or significance of call signatures (or lack of such signature) through their consumer displays.”)

<sup>7</sup> See, e.g., *Telephone Number Portability Order*, Third Report and Order, 13 FCC Rcd 11701 (1998). The Commission sought comment on cost recovery mechanisms in its SHAKEN/STIR NOI. *Call Authentication Trust Anchor*, Notice of Inquiry, 32 FCC Rcd 5988, 6000, ¶ 47 (2017) (“SHAKEN/STIR NOI”).

SHAKEN/STIR for carriers that use TDM technology or where TDM is used during part of the call flow.<sup>8</sup>

Most critically for CCA members, the framework does not have a protocol or standards for assuring the highest level of attestation – or perhaps any ability to sign at all – for certain types of legitimate calls made from enterprise customers, for example when the enterprise utilizes several carriers or the signing provider did not assign to the caller the number used in the caller ID. The lack of a process to address common enterprise calling use cases potentially puts the service providers serving those enterprises, particularly smaller providers, at a disadvantage if their enterprise customers’ calls are blocked or adversely labelled because they are unsigned or signed at a lower level of attestation.

#### **B. Critical Aspects of the Framework Remain Under Unresolved**

As the NANC report recognized, “[a]lthough SHAKEN provides a mechanism for call authentication, this system does not establish call validation treatment applications (e.g., call blocking or certified identify).”<sup>9</sup> These “next steps,” the NANC recognized, are required to extend the framework to “either enhanced service providers services, or third-party applications as enhancements to traditional telephone services.” These next steps remain to be taken and until they are, participation by “enhanced service providers” serving enterprise customers, which would appear to include CCA members that provide over-the-top unified communications services, may not be feasible or effective. To be clear, CCA members recognize that remaining outside of the framework as more and more providers participate may put them at a competitive

---

<sup>8</sup> The IETF has recently issued a draft document describing, at a high level, a potential solution using out of band signaling and a new service it calls “call placement service.” See STIR Out-of-Band Architecture and Use Cases, draft ietf-stir-oob-05 (July 8, 2019) available at <https://datatracker.ietf.org/doc/draft-ietf-stir-oob/> (last visited July 23, 2019).

<sup>9</sup> NANC Report at 5.

disadvantage.<sup>10</sup> There is thus every incentive to participate in the framework. But the framework must also enable their participation, and there is the rub.

The problem faced by CCA members, and many other IP-enabled providers that serve enterprise customers, was recently described in an Internet Engineering Task Force (“IETF”) draft report. This draft, released on July 8, 2019, describes the problem of certifying calls from non-carrier entities, such as over-the-top VoIP providers or their enterprise customers. The draft discusses a potential solution that would allow holders of SHAKEN/STIR certificates, primarily carriers, to delegate “a subset of that certificate’s authority to another party.”<sup>11</sup> That party could then sign under its delegated certificate and authenticate the call. This certificate delegation concept supersedes another proposed solution to these problems that was known as telephone number proof of possession, or TNPoP, that had been under consideration until recently.<sup>12</sup>

The IETF draft observes that the most pressing use case for certificate delegation occurs when an outbound enterprise call is carried by a provider that does not control the calling number.<sup>13</sup> As described in the draft, this may occur when an enterprise uses a number of

---

<sup>10</sup> See NANC Report at 16 (“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 calls since they would otherwise risk that many of their customers’ calls will be rejected, putting that provider at a distinct competitive disadvantage”).

<sup>11</sup> STIR Certification Delegation, draft-ietf-stir-cert-delegation-00 (July 9, 2019) at 2 (“STIR Cert. Delegation”) available at <https://tools.ietf.org/html/draft-ietf-stir-cert-delegation-00> (last visited July 18, 2019). The concept of delegation was discussed in the Commission’s SHAKEN/STIR notice of inquiry. SHAKEN/STIR NOI, 32 FCC Rcd at 5997, ¶ 34 (2017).

<sup>12</sup> See, e.g., Letter from David Morken, Bandwidth, to Honorable Ajit V. Pai, FCC, WC Docket No. 17-97, CG Docket 17-59 (filed November 19, 2018) (“Bandwidth Nov. 2018 Letter”) (noting that “the industry’s efforts to accurately identify valid end-user originated traffic as distinct from illegal robocalls, will hinge critically upon the adoption of a set of [TNPoP] standards and best practices alongside SHAKEN/STIR.”). Bandwidth further noted that without TNPoP many innovative communications providers “will be discriminated against.” *Id.* at 2. Bandwidth recently reiterated these concerns in a letter to Commissioner Starks stating that “[e]nsuring that illegal robocall prevention coexists with effective traffic delivery of legal calls across the communications ecosystem will depend critically upon the adoption of a set of additional supplemental standards and best practices to the current SHAKEN/STIR specifications.” Letter from David Morken, Bandwidth, to Honorable Geoffrey Starks, FCC, WC Docket No. 17-97, CG Docket 17-59 (filed July 10, 2019).

<sup>13</sup> STIR Cert. Delegation at 3 (“The most pressing need for delegation in STIR arises in a set of use cases where a caller wants to use a particular calling number, but for whatever reason, their outbound calls will not pass through the authentication service of the service provider that controls the number.”)



different transport providers and chooses which provider to use for any given call based on the least cost provider.<sup>14</sup> The draft also describes another common calling scenario involving “legitimate spoofing” such as “where a user wants to be able to use the main call-back number for their business as a calling party number, even when the user is away from the business.”<sup>15</sup> Additionally, many CCA members’ services involve several service providers: the CCA member company providing OTT VoIP, carrier partners that may provide telephone numbers and thus control the numbering resource, and the underlying broadband provider that may physically transport the outbound call.

The IETF draft suggests that these types of use cases could be addressed through certificate delegation, but without that sort of solution, legitimate calls could be indistinguishable from malicious spoofing:

These sorts of use cases could be addressed if the carrier who controls the numbering resource were able to delegate a credential [*e.g.*, a telephone number or range of telephone numbers] that could be used to sign the calls regardless of which network or administrative domain handles the outbound routing for the call. In the absence of something like a delegation mechanism, outbound carriers may be forced to sign calls with credentials that do not cover the originating number in question. Unfortunately, that practice would be *difficult to distinguish from malicious spoofing*, and if it becomes widespread, it could erode trust in STIR overall.<sup>16</sup>

The IETF working group draft report’s concern that the signing of otherwise legitimate calls by entities that do not control the number would be indistinguishable from malicious spoofing raises a key issue. The Further Notice seeks comment on whether to establish a safe harbor for malicious spoofing on the belief that “the vast majority” of such calls would be

---

<sup>14</sup> Id. (“One example would be an enterprise that places outbound calls through a set of service providers, for each call choosing a provider based on a least-cost routing algorithm or similar local policy. The enterprise was assigned a calling number by a particular service provider, but some calls originating from the number will go out through other service providers.”)

<sup>15</sup> Id.

<sup>16</sup> Id. at 2-3 (emphasis added).

“illegitimate.”<sup>17</sup> The Further Notice does not provide any information on how the Commission believes that malicious spoofing could be determined but the IETF draft suggests that it may be much more difficult than the Commission assumes. Of course, the alternative to signing without appropriate credentials may be that the outbound carrier does not sign the call at all, or signs with a lower level of attestation. Depending on how such calls are treated by the terminating provider (which remains an open issue), the call may not be forwarded to the recipient, or the call may be adversely labeled, which puts the OTT VoIP provider in a disadvantageous position.

In light of these concerns, CCA respectfully urges the Commission to exercise caution in adopting any safe harbors based on any SHAKEN/STIR information, including the lack of a signature or a lesser level of attestation, until a set standards and best practices concerning the signing of enterprise-originated calls have been adopted and proven workable. The Commission initially assumed that the SHAKEN/STIR framework would be implemented in three phases. The first phase would entail development of the SHAKEN/STIR standards. The second phase would be the establishment of the governance structure. The third phase would entail presentation of SHAKEN/STIR information to end users. All of these phases should be fully implemented, and none are as of yet, before authorizing call blocking.

For the same reasons, it would be premature to establish safe harbors based on the nature or category of voice providers.<sup>18</sup> The Further Notice asks, for example, whether a safe harbor should apply for voice providers that do not appropriately sign calls or do not participate in trace back efforts. As noted above, however, there may be legitimate reasons why some providers are unable to sign calls.

---

<sup>17</sup> Further Notice at ¶ 51 (proposing a safe harbor for blocking calls that fail Caller ID authentication, that is, “when the attestation header has been maliciously altered or inserted”).

<sup>18</sup> Id. at ¶ 55.

The Further Notice recognizes that smaller voice providers may need more time to implement SHAKEN/STIR and thus seeks comment on the economic impact of safe harbors. The Commission's concern, however, appears limited to small rural providers, especially those participating in the universal service high-cost fund. This is too narrow. Small rural carriers are not the only the service providers that may need more time to implement SHAKEN/STIR. As amply demonstrated above, a broad range of smaller, competing providers will need more time to implement the framework, both because of fewer resources, but also because the framework as currently constituted does not afford them the opportunity to fully participate.

The Commission may wish to provide guidance to the SHAKEN/STIR governance authority, or direct the authority, to devise a more fulsome plan to phase in adoption of the framework across the communications ecosystem. As noted above, the Commission assumed a three phase approach to implementation. As part of this phased approach, the Commission could establish further timelines and testing procedures for concepts such as certificate delegation or out-of-band signaling that would enable the broadest possible participation in the framework.<sup>19</sup> These mechanisms can be invoked and tested but without acting on the authentication information generated until the mechanisms are shown to be workable and efficacious.

### **III. Safe Harbors, if Adopted, Should Require Implementation of Effective and Timely Mechanisms to Promptly Address Inadvertent or Erroneous Blocking or Labeling of Legitimate Calls**

The Further Notice seeks comment on mechanisms to address the blocking of legitimate calls.<sup>20</sup> This is critically important, especially if the Commission adopts safe harbors that remove the possibility of adverse consequences for blocking legal calls. The Commission acknowledged

---

<sup>19</sup> See, e.g., Comments of Neustar, Inc., CG Docket No. 17-97, at 2 (filed August 14, 2017) ("Neustar NOI Comments") (suggesting the Commission establish milestones and timelines for testing and validation). Certain timelines and milestones have been set relating to the governance structure.

<sup>20</sup> Further Notice ¶¶ 58, 70.

the importance of these mechanisms in the accompanying Declaratory Ruling by requiring, as part of a “reasonable call-blocking program,” that the blocking provider identify a point of contact for legitimate callers to report erroneous blocking and to implement “a mechanism for such complaints to be resolved.”<sup>21</sup> The Commission also encouraged voice providers to develop a mechanism to notify callers that their calls have been blocked.<sup>22</sup> Notification of blocking is critical. Callers need to know that their calls are being rejected due to blocking and by whom so that they can promptly invoke the blocking entity’s mechanisms to reverse blocking of legitimate calls.

These are important steps but the Commission should go further than simply encouraging the adoption of such mechanisms. It should require that any voice provider blocking calls implement a mechanism to reverse the blocking of legal calls. The Commission should also provide additional specificity regarding such a mechanism, while not mandating a one-size-fits-all solution. Voice providers should, for example, adopt and publicize a timeline for resolution as well as have a process for the prompt unblocking of a call upon a reasonable showing by the caller that it is a legitimate enterprise authorized to use the numbers appearing in the caller ID. Additionally, notification of blocking should be required, not simply encouraged, and the notification should take the form of intercept message or SIP code. The Commission noted that a SIP response code “specifically intended to notify calling parties that an intermediary has rejected their call attempt is currently in process with the IETF.”<sup>23</sup>

As blocking becomes more and more prevalent, the Commission may wish to explore a more uniform process for immediate unblocking, for example, through the use a national

---

<sup>21</sup> Declaratory Ruling ¶ 38.

<sup>22</sup> Id.

<sup>23</sup> Further Notice n. 106.

database administrator, such as used for number porting. Authorized and trusted providers could immediately white list or black list numbers in the database.

#### **IV. International Calls Should Not Automatically Be Blocked**

Many fraudulent or illegally spoofed calls originate in foreign countries.<sup>24</sup> Domestic providers that receive intentional calls on their networks for termination may have no information regarding the originating caller or whether the caller has any authority to use the calling party number. The SHAKEN/STIR framework proposes to address this problem through the gateway attestation that is to be provided by the first domestic provider that receives the call on its network. The gateway or C-level attestation simply certifies that the call has entered that provider's network. It is unclear how C-level attestations would be presented to the domestic called party, if at all.

CCA has many foreign companies that provide cloud-based VoIP and enterprise communications services to legitimate companies located in Europe and Asia. These companies would, of course, be concerned if their calls to the U.S. were blocked based on the level of attestation. While countries have expressed interest in the SHAKEN/STIR model, global implementation remains a long-term goal. CCA would urge the Commission not to authorize blocking based solely on the foreign origin of the call. Determining whether a foreign-originated call is fraudulent or illegal will require review of various indicia. Moreover, foreign callers and their service providers must also have access to mechanisms to reverse erroneous call blocking.

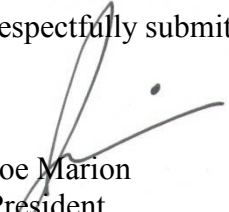
#### **V. CONCLUSION**

For the reasons set forth above, CCA respectfully urges the Commission to refrain from authorizing safe harbors for blocking labeling calls based on SHAKEN/STIR information until the framework has been fully implemented.

---

<sup>24</sup> Id. at ¶ 82.

Respectfully submitted,



Joe Marion  
President  
Cloud Communications Alliance  
131 NW 1st Avenue  
Delray Beach, FL, USA 33444  
(561) 232-3891

July 24, 2019

19501067