February 20, 2023

***Ex Parte* Notice**

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
45 L Street, N.E.
Washington, D.C., 20554

RE: Call Authentication Trust Anchor, WC Docket No. 17-97

Dear Ms. Dortch:

On Thursday, February 16, 2023, the undersigned on behalf of NTCA–The Rural Broadband Association ("NTCA"),[1] David Frigen, Chief Operating Officer with Wabash Communications Co-op[2] and Alec Fenichel, Chief Technology Officer with TransNexus[3] (the "Rural Representatives") met with the following Federal Communications Commission (the "Commission") staff: Zachary Ross, Assistant Chief of the Wireline Competition Bureau's ("WCB") Competition Policy Division, Kenneth Carlberg, Chief Technologist with the Public Safety and Homeland Security Bureau, and Jesse Goodwin, Connor Ferraro, Andrea Capone and Meghan Bryan with the WCB. The parties discussed the record compiled in response to the Notice of Inquiry ("NOI")[4] issued by Commission seeking input on the agency's next steps in its ongoing implementation of the TRACED Act,[5] in particular, the prevalence of non-Internet Protocol ("IP"), or Time-division multiplexing ("TDM"), facilities within voice networks.

In the meeting, the Rural Representatives emphasized the need to move forward with implementation of technical standards for caller-ID authentication over non-IP networks that meet the definition of "reasonably available" as set forth by the Commission in 2020.[6] The parties further stated that either delaying such implementation or failing to address IP interconnection gaps in the exchange of voice traffic will perversely perpetuate the existence of non-IP facilities that act as a considerable gap in the STIR/SHAKEN ecosystem. Thus, Commission action to require implementation of these standards or to further IP interconnection – and in a way that does

[1] NTCA represents approximately 850 providers of high-quality voice and broadband services in the most rural parts of the United States; historically, these have been referred to as rural local exchange carriers or "RLECs." In addition to voice and broadband, many NTCA members provide wireless, video, and other advanced services in their communities.
[2] Established in 1952, Wabash Communications (Wabash) is a rural incumbent Local Exchange Carrier and Telecommunications Cooperative located in South Central Illinois, delivering traditional telecommunications services to its rural members and customers. Wabash also represents over 850 independent telecommunications providers of NTCA–The Rural Broadband Association while serving on the STI-GA Board of Directors, and serves on the ATIS Non-IP Call Authentication Task Force ("NIPCA").
[3] TransNexus provides software to manage and protect telecommunications networks.
[4] Call Authentication Trust Anchor, WC Docket No. 17-97, Notice of Inquiry, FCC 22-81 (rel. Oct. 28, 2022) ("NOI").
[5] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, § 4(b)(1)(B) (2019) (codified at 47 U.S.C. § 227b(b)(1)(B)) (TRACED Act).
[6] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, FCC 20-136 (rel. Oct. 1, 2020) ("*Second Caller ID Authentication Report and Orde*r"), ¶ 68.

not increase voice rates for rural consumers or put call reliability or quality in question – is necessary to break this unfortunate logjam.

Non-IP Voice Service Facilities Are a Considerable Gap in the STIR/SHAKEN Ecosystem.

As an initial matter, the parties stated that the record in this proceeding demonstrates that the continued presence of "non-IP" voice networks results in a considerable "gap" in the STIR/SHAKEN ecosystem. As the comments of the Cloud Communications Alliance,[7] the Competitive Carriers Association,[8] the VON Coalition[9] and NCTA[10] show, the gap – which prevents end-to-end caller-ID authentication – is one that is not limited to NTCA members, to rural or small providers, or traditional wireline operators, but rather is widespread across the voice service industry due primarily to the presence of intermediate switches and interconnection facilities that remain non-IP. This persistent gap in key parts of network hierarchies prevents carriers of all sizes and technologies from successfully authenticating caller-ID on an end-to-end basis using STIR/SHAKEN.

Most importantly, the non-IP gap precludes successful authentication even when a provider has the ability to originate/terminate calls in IP – other operators' non-IP facilities in the path of perhaps millions of calls per day mean that authentication information is lost in transit through no fault of the originating or terminating providers. Indeed, the substantial investments that NTCA members and many operators of the kinds cited above have made in IP-enabled and STIR/SHAKEN-capable networks are defeated because of other operators' non-IP facilities – an inarguably large "non-IP" gap in the authentication ecosystem. This is therefore not a problem that can be solved by IP-enabled providers simply investing more in their networks and STIR/SHAKEN authentication technologies. Moreover, pointing to "an unprecedented wave of privately funded and government-backed broadband deployment"[11] is utterly misplaced and an attempt at misdirection – the issue is not *broadband* investment but rather investment (or a lack thereof) in *voice routing capabilities* to ensure they can authenticate calls as contemplated by the TRACED Act.

The Rural Representatives then observed that the assertion that the non-IP gap is "small"[12] and thus tolerable misses the mark for several reasons. For one, this insinuates that the Commission should accept the fact that a large number of voice providers must invest in STIR/SHAKEN only to see it not work as intended because of the persistent presence of other operators' non-IP facilities through which calls are routed. This is not only a waste of funds invested, but far more importantly, it could still leave millions of consumers without access to the benefits of caller-ID authentication that the TRACED Act specifically sought to ensure. In addition, the value of blocking tools and traceback efforts to which USTelecom points as being effective and thus

---

[7] Comments of the Cloud Communications Alliance ("Alliance"), WC Docket No. 17-97 (fil. Dec. 12, 2022), p. 2.
[8] Comments of the Competitive Carriers Association, WC Docket No. 17-97 (fil. Dec. 12, 2022), p. 4.
[9] Comments of the Voice on the Net Coalition ("VON"), WC Docket No. 17-97 (fil. Dec. 12, 2022), p. 1.
[10] Comments of NCTA – The Internet & Television Association ("NCTA"), WC Docket No. 17-97 (fil. Dec. 12, 2022), p. 2.
[11] Comments of USTelecom – The Broadband Association ("USTelecom"), WC Docket No. 17-97 (fil. Dec. 12, 2022), p. 10.
[12] *Id*. p. 3.

negating the need for authentication across all networks/calls[13] would be more effective if non-IP networks did not stand in the way of so many calls being authenticated end-to-end.

Arguments that the non-IP gap is "small" or that the Commission need not take any action here ignore the TRACED Act – the Commission has the legal authority, and in fact an obligation, to ensure widespread caller-ID authentication.

The Rural Representatives noted that the Commission not only has the legal authority to address the non-IP gap described above, but in fact an obligation under the TRACED Act to ensure widespread caller-ID authentication. Specifically, the TRACED Act does not allow for a permanent or even long-term TDM exemption. To the contrary, section 4(b)(5)(B) states that:

> Subject to subparagraphs (C) through (F), for any provider or class of providers of voice service, or type of voice calls, only to the extent that such a provider or class of providers of voice service, or type of voice calls, materially relies on a non-internet protocol network for the provision of such service or calls, the Commission shall grant a delay of required compliance under subparagraph (A)(ii) ***until*** a call authentication protocol has been developed for calls delivered over non-internet protocol networks and is reasonably available.[14]

In its interpretation of this language, the Commission quoted this section and then stated that, based on the TRACED Act, "we grant [an extension] from implementation of caller ID authentication…for the parts of a voice service provider's network that rely on technology that cannot initiate, maintain, and terminate SIP calls ***until*** a solution for such calls is reasonably available."[15] As discussed further below and as the record in response to the NOI indicates, two technical standards for caller-ID meet the "reasonably available" test.

In addition, the Rural Representatives pointed to the Commission's previous reliance on 251(e) of the Communications Act and the Truth in Caller-ID Act. As the Commission stated in the *Second Caller ID Authentication Report and Order*, requiring "voice service providers [to take] 'reasonable measures' to deploy an effective caller ID authentication framework in the non-IP portions of their networks will help to prevent the fraudulent exploitation of NANP resources by permitting those providers and their subscribers to identify when caller ID information has been spoofed."[16] With respect to the Truth in Caller-ID Act, in adopting the provisions for "reasonable measures" to authenticate calls in non-IP networks, the Commission noted that "[g]iven the constantly evolving tactics by malicious callers to use spoofed caller ID information to commit fraud, we find that the rules we adopt today are necessary to enable voice service providers to help prevent these unlawful acts and to protect voice service subscribers from scammers and bad actors."[17]

Against this backdrop, the Rural Representatives reiterated that requiring those materially relying on non-IP facilities to take "reasonable measures" to find a solution was not intended as a

[13] *Id*., p. 4.
[14] TRACED Act § 4(b)(5)(B).
[15] *Second Caller ID Authentication Report and Order,* ¶ 38.
[16] *Id*., ¶ 34.
[17] *Id*., ¶ 35.

permanent pass on authentication – instead, this was clearly intended as a stopgap by the Commission to apply ***until*** a solution was "reasonably available." Now that two standards meet that test, the Commission should move forward with implementation of those standards, and the TRACED Act, Section 251(e), and the Truth in Caller-ID Act all provide the agency with the legal foundation to do so.

Finally, with respect to legal authority, the Rural Representatives stated that no party disputed the Commission's legal authority in responding to the NOI.

Two published and vendor-supported non-IP standards meet the test the FCC set forth in the Second Report and Order, and operators can use them today to close the non-IP gap.

Two technical standards for non-IP call authentication are "reasonably available."

Turning to the non-IP authentication standards, the Rural Representatives observed that the Commission previously committed to revisiting the non-IP extension at a point when a solution meets the test of being "reasonably available."[18] This was further defined in the *Second Caller ID Authentication Report and Order* as a solution being "fully developed and finalized by industry standards" and when "the underlying equipment and software necessary to implement such protocol is available on the commercial market."[19] As the record indicates, two non-IP authentication standards meet this test.

As the NOI acknowledges, two technical standards that allow for the use of STIR/SHAKEN caller ID authentication protocols over non-IP facilities have been published – these were discussed and finalized by the NIPCA standards body formed under the auspices of ATIS and with a membership that is comprised of a representative cross-section of the overall voice service provider and vendor community.[20] Like NTCA, a number of parties point to the Out of Band ("OOB") non-IP authentication solution as "commercially available," thus meeting the "reasonably available" test. It is also important to note that this OOB solution (ATIS-1000096) is available via at least three vendors. The "in-band" or "Shaken over TDM" (ATIS-1000095.v002) standard is commercially available as well – when referring to both technical standards, TelcoBridges states that it, "supports both mechanisms as a policy matter and offers technology solutions for both."[21]

Security concerns raised by two parties are misplaced, having been addressed in the NIPCA.

The Rural Representatives first noted that it is misleading to assert that "security" concerns have not been a part of the NIPCA discussions or have not been successfully addressed. The issue was indeed discussed and addressed by the NIPCA, and any assertion that the issue remains open is baseless. As to the substance of the concern, while Verizon claims that "[s]ince STIR/SHAKEN

[18] *Id*., ¶ 32.
[19] *Id*., ¶ 68.
[20] NTCA, Wabash and Transnexus are members of the NIPCA. ATIS, Non-IP Call Authentication Task Force – Members page, available at: https://www.atis.org/committees-forums/ptsc/non-ip-call-authentication-task-force-members/
[21] Comments of TelecoBridges, WC Docket No. 17-97 (fil. Dec. 12, 2022), p. 4.

identity rules are being applied out-of-band, nothing prevents an attacker from hijacking the stored identity credentials,"[22] this specific issue was raised and addressed in both ATIS 1000097.v002 and IETF RFC 8816.[23] These documents found that the security concern to which Verizon points could only be exploited in very narrow circumstances, and included mitigation techniques to address such concerns.[24]

With respect to the assertion that the OOB solution creates a "CPNI vulnerability," this claim is misplaced as well. This concern was addressed by the NIPCA during the development of ATIS-1000096, which states that "only authorized members of the SHAKEN ecosystem have access to the CPS network."[25] Thus, only those approved and trusted service provider representatives would have access to CPNI – and the breathless claim that "private investigations and domestic abusers" will have access to this information is simply incorrect.

Denial of service attack concerns are unfounded.

Turning to additional criticism of the OOB solution, the Rural Representatives stated that STI-Call Placement Service ("CPS") operators currently utilize protections against denial-of-service attacks similar to how parties involved in the In-Band IP-SHAKEN environment do today. In short, the potential for these denial of service attacks is not unique to OOB and is in fact a possibility with current IP-SHAKEN authentication being used today. A Transnexus description of its STI-CPS architecture and its included denial-of-service attack protections were also discussed.[26]

The Out-of-Band Solution is being used today to authenticate caller-ID on an end-to-end basis.

The Rural Representatives then turned to a discussion of the non-IP standards in use today. As Wabash Communications has repeatedly stated and reiterated in the meeting, the company has effectively implemented the OOB solution and has successfully exchanged authenticated voice traffic with other several other operators also using that solution. Another group of voice service providers have, like Wabash, indicated their use of this standard to successfully authenticate calls on an end-to-end basis.

The Out-of-Band Solutions from various vendors are interoperable and thus concerns about their supposed "proprietary" nature are misplaced.

The alleged "proprietary"[27] nature of existing OOB solutions is not a barrier to widespread use/scaling of this authentication standard. Put another way, two operators utilizing different OOB solutions from different vendors can successfully exchange authentication information.

---

[22] Comments of Verizon, WC Docket No. 17-97 (fil. Dec. 12, 2022), appendix A.
[23] ATIS-1000097.v002, Alternatives for Call Authentication for Non-IP Traffic (Sep. 2, 2022), p. 12-13.
[24] *Id*.
[25] Comments of TransNexus, WC Docket No. 17-97 (fil. Dec. 12, 2022). p. 10.
[26] STIR/SHAKEN Out-of-Band Call Placement Service, available at https://transnexus.com/shaken-call-placement-service/.
[27] USTelecom, p. 16.

Implementation of the Non-IP standards will not impede the IP transition; indeed, the Commission failing to take action to close the non-IP gap will only perpetuate its existence.

As an initial matter, the Rural Representatives urged the Commission to reject the notion that a mandate to implement the non-IP authentication standards would impede the IP transition. To the contrary, *it is more likely that such a mandate will further the IP transition*, by prompting those desiring, at nearly all costs, to avoid investing in their non-IP facilities to seek out a reasonable path to upgrade to IP networks instead of implementing non-IP authentication solutions. Moreover, the Commission should keep in mind that those using this excuse have had over three years since the TRACED Act gave these operators a clear choice to upgrade to IP or use a non-IP standard once developed. These are also the same providers that issued urgent warnings several years ago stating that mandates governing TDM facilities, in the context of the Commission's 988 proceeding, were ill-advised. Despite claims there that ancient and no longer vendor-supported TDM facilities were incapable of compliance with a requirement to route calls placed to 988 to the suicide hotline,[28] much of this equipment remains in their networks today.

NTCA submits therefore that the worst thing the Commission can do, in terms of furthering the ongoing IP transition and protecting consumers, is to do nothing. Pursuant to the rules adopted in the *Second Caller ID Authentication Report and Order* (Section 64.6303),[29] providers that materially rely on non-IP facilities must either (1) upgrade their facilities to IP or (2) participate in a standards body working on a non-IP solution. With two such standards now developed and meeting the "reasonably available" test, and with security concerns already addressed, it is unclear what is left to be worked upon by a standards body. Indeed, the two standards are "closed" pursuant to the practices used by NIPCA and other standards bodies. Unfortunately, the Commission's rules as currently worded effectively incent endless discussion of already published standards. *Put another way, this state of affairs is the real impediment to the IP transition – the rules require nothing more than either upgrading of networks to IP or unending recurring discussion of standards already adopted.* The Rural Representatives therefore urged the Commission to recognize that inaction here is the true impediment to the IP transition and widespread caller-ID authentication.

The Rural Representatives then stated that a non-IP mandate could be unnecessary, however, if the Commission took meaningful action to facilitate a transition away from non-IP interconnection arrangements – but any such efforts must take account of the potential cost shifts that could harm rural consumers in doing so. While the current model of voice interconnection apportions costs for transport and traffic exchange between RLECs and other operators in a manner that helps to promote reasonable comparability of price and quality in the offering of voice services to urban and rural users alike, this long-standing and equitable apportionment could be turned on its head if

[28] Comments of USTelecom, WC Docket No. 18-336 (fil. Feb. 14, 2020), pp. 13-14; Reply comments of CenturyLink, WC Docket No. 18-336 (fil. Mar. 16, 2020), pp. 5-6.

[29] *Second Caller ID Authentication Report and Order*, ¶ 24. *See also*, 47 C.F.R. § 64.6303 (stating that a voice service provider "shall either: (a) upgrade its entire network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework as required in 47 CFR 64.6301 throughout its network; or (b) maintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non Internet Protocol caller identification authentication solution, or actively testing such a solution.").

IP interconnection is implemented at a few POIs scattered in urban areas across the country that are distant from more rural markets. Absent Commission attention to this economic dynamic in any action to facilitate IP interconnection, smaller rural operators would in all likelihood be forced to pay for "voice transit" (i.e., transport) to reach these distant POIs and pass such costs onto small rural customer bases.

That said, the Commission can spur IP interconnection and protect rural consumers via a simple "hold harmless" declaration that any RLEC will not be financially responsible as a matter of cost for more than it bears today in routing such calls through existing TDM-based interconnections with other voice service providers. The preservation of existing well-known and well-defined constructs that would result from such a Commission declaration should in fact expedite the implementation of IP voice interconnection and the ensuing implementation of STIR/SHAKEN across all networks because all parties' relative responsibilities would be clearly defined in advance as a default. In fact, those operators with whom RLECs exchange traffic at tandems today would perhaps take the regulatory certainty this provision would produce and, knowing the "basic rules of the road," would be more likely to offer IP interconnection where they have not before.

In closing, the Rural Representatives stated that the failure to act here will translate to many calls being sent all across the nation without caller-ID authentication, a scenario that seemingly has no end in sight – as noted above, those materially relying on non-IP facilities have little incentive to move on from them. The failure to require those with non-IP facilities to do anything more than continue discussing already "reasonably available" standards will only perpetuate this state of affairs. In the end, Commission action here should not be limited to a mandate for implementation of these standards, but rather provide operators with a choice – to upgrade their networks and interconnect on reasonable terms and conditions (such as those described above) in IP or to implement non-IP solutions where they choose not to invest in such upgrades or to provide reasonable IP-based interconnection.

Thank you for your attention to this correspondence. Pursuant to Section 1.1206 of the Commission's rules, a copy of this letter is being filed via ECFS.

Sincerely,
/s/ *Brian Ford*
Brian Ford
Vice President–Federal Regulatory
NTCA–The Rural Broadband Association

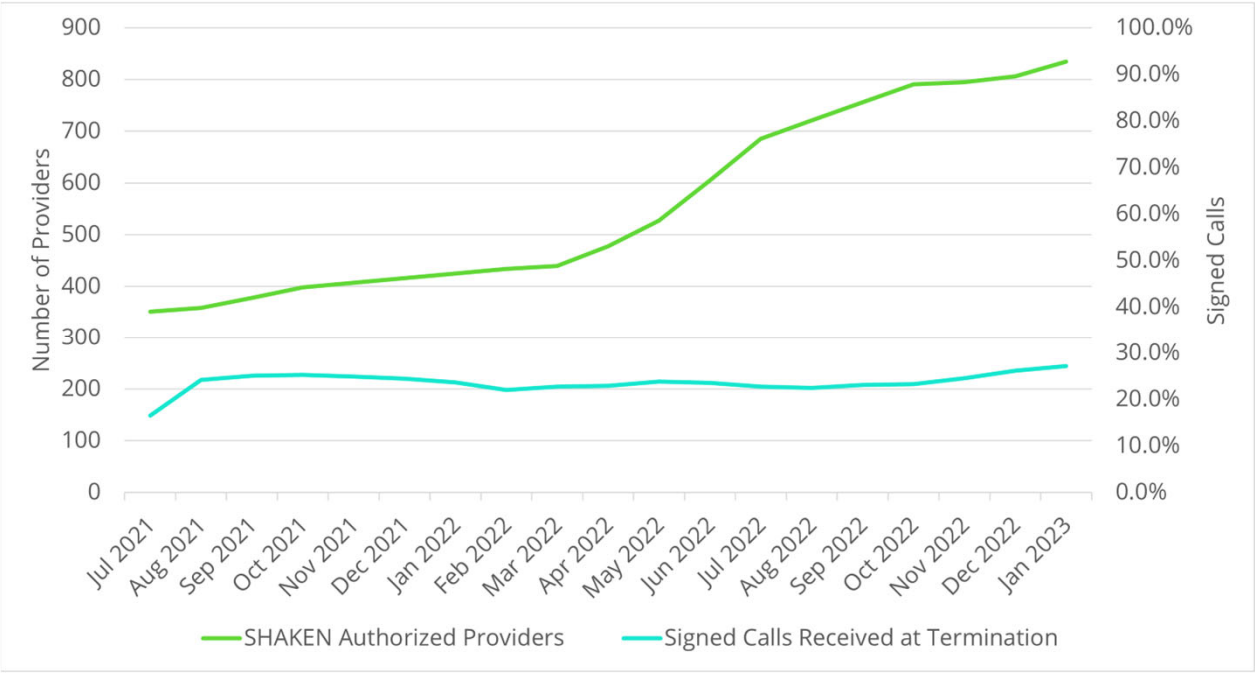
cc: Zachary Ross
Connor Ferraro
Jesse Goodwin
Kenneth Carlberg
Andrea Capone
Meghan Bryan

Agenda

- The “non-IP gap” in the STIR/SHAKEN ecosystem is considerable.
- The Commission has legal authority to close the gap.
- The TRACED Act instructs the Commission to pursue widespread authentication.
- Non-IP SHAKEN standards are fully developed and solutions are reasonably available.
- Verizon’s security concerns have been addressed in NIPCA and IETF.
- Nothing stands in the way of the Commission moving from development to implementation of these standards.

Non-IP is a significant problem

- TransNexus has been publishing monthly STIR/SHAKEN statistics gathered from over 100 voice service providers
- Many of the service providers are fully IP (including interconnects)
- Fewer than 30% of received calls are signed, we suspect this is primarily due to non-IP



The Commission has legal authority

- The TRACED Act gives the Commission authority to require a provider of voice service to take reasonable measures to implement an effective call authentication framework in the non-internet protocol networks of the provider of voice service: TRACED Act § 4(b)(1)(B).
- Section 251(e) of the Communications Act of 1934 as amended provides the Commission with the authority to set policies to help prevent fraudulent exploitation of the North American Numbering Plan resources: 47 U.S.C. § 251(e). This authority provides jurisdiction to include intermediate providers that own and operate many of the non-IP segments along call paths in the U.S., where, absent the Commission's exercise of this authority, call authentication information would be lost.
- The Truth in Caller ID Act gives the Commission legal authority to set rules to make unlawful the spoofing of caller ID with the intent to defraud, cause harm, or wrongfully obtain anything of value: 47 U.S.C § 227(e)(1). This gives the Commission authority to mandate that intermediate providers either transition to IP or adopt a framework that will minimize the frequency with which illegally spoofed scam calls will reach consumers.

The Commission has undisputed legal authority

- TransNexus and Cloud Communications Alliance stated that the TRACED Act gives the Commission legal authority for non-IP call authentication in NOI comments.
- TransNexus and Cloud Communications Alliance stated that the Communications Act of 1934 and the Truth in Caller ID Act give the Commission legal authority to place obligations on intermediate providers in NOI comments.
- No one disputed these statements in NOI reply comments.

Current rules incentivize endless working group activity

47 CFR 64.6303 Caller ID authentication in non-IP networks:

"(a) Except as provided in §§ 64.6304 and 64.6306, not later than June 30, 2021, a voice service provider shall either:

(1) Upgrade its entire network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework as required in § 64.6301 throughout its network; or

(2) Maintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-internet Protocol caller identification authentication solution, or actively testing such a solution.

(b) Except as provided in § 64.6304, not later than June 30, 2023, a gateway provider shall either:

(1) Upgrade its entire network to allow for the processing and carrying of SIP calls and fully implement the STIR/SHAKEN framework as required in § 64.6302(c) throughout its network; or

(2) Maintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-internet Protocol caller identification authentication solution, or actively testing such a solution."

The non-IP standards are complete

- The Non-IP Call Authentication (NIPCA) Task Force uses projects with issue statements to determine what work to complete
- The project to develop the non-IP standards (PTSC Issue 0158) has been closed
- Further development of the non-IP standards is not expected
- A new project (PTSC Issue 0163) was created on 08-26-2022 to develop a second technical report ostensibly to discuss viability
- The new technical report appears to be a stalling tactic by the intermediate carriers to avoid § 64.6303 (a)(1)

The TRACED Act instructions the Commission to remove the delay

TRACED Act § 4(b)(5)(B):

"DELAY OF COMPLIANCE REQUIRED FOR CERTAIN NONINTERNET PROTOCOL NETWORKS.—Subject to subparagraphs (C) through (F), for any provider or class of providers of voice service, or type of voice calls, only to the extent that such a provider or class of providers of voice service, or type of voice calls, materially relies on a non-internet protocol network for the provision of such service or calls, the Commission shall grant a delay of required compliance under subparagraph (A)(ii) until a call authentication protocol has been developed for calls delivered over non-internet protocol networks and is reasonably available."

Non-IP SHAKEN is developed and reasonably available

- Developed
  - 2021-07-20 – ATIS-1000096 published
  - 2022-08-30 – ATIS-1000095.v02 published
  - 2022-09-08 – ATIS-1000097.v02 published
  - 2022-11-15 – ATIS Robocalling Testbed adds support for ATIS-1000096
- Reasonably available
  - TransNexus provides ATIS-1000096 compliant software
  - net number provides ATIS-1000096 compliant software
  - TransNexus provides an STI-CPS
  - net number provides an STI-CPS

Verizon's 1st security concern has been addressed

ATIS-1000097.v002 A.1 "Security considerations":

"Leverages the extensive security analysis performed in the IETF [Ref 5]. Drastically simplifies the security requirements by limiting access to only Secure Telephone Identity Policy Administrator (STI-PA)-approved service providers. PASSporTs (as defined in RFC 8225 [Ref 101]) have minimal replay attack prevention. The combination of calling number, called number, and approximate timestamp are all that bind a PASSporT to a call. An attacker with timely access to a PASSporT can perform a replay attack. Note that the attacker must use the same calling number and called number as the original call for the replay attack to result in a successful verification. Out-of-Band SHAKEN (as defined in ATIS1000096 [Ref 3]) potentially offers an additional attack surface that can be used to perform replay attacks. With Out-of-Band SHAKEN, an attacker may not need timely access to the PASSporT if certain conditions are met. The attacker must still have timely knowledge of a call occurring from a given calling number to a given called number or have a method of triggering a call from a given calling number to a given called number (e.g., triggering a Multi-Factor Authentication (MFA) phone call after compromising a password). The attacker must be able to originate a call with the given calling number (meaning the attacker's originating service provider must not prevent the attacker from spoofing a calling number). The original call must use TDM and the service provider who converts the call from SIP to TDM (or the originating service provider if the call originates TDM) must publish the PASSporT to the STI-CPS (note that the attacker does not control this behavior nor have any way of knowing it is occurring). The attacker's call must also use TDM, but in this case the service provider who converts the call from SIP to TDM (or the originating service provider if the call originates TDM) must not publish the PASSporT to the STI-CPS (note that the attacker does not control this behavior nor have any way of knowing it is occurring). For the attacker's call, the service provider who converts the call from TDM to SIP (or the terminating service provider if the call terminates TDM) must retrieve the PASSporT from the STI-CPS (note that the attacker does not control this behavior nor have any way of knowing it is occurring). Due to the number of conditions that must be met, the attacker will likely need to originate a large volume of calls to successfully perform a single replay attack. The large volume of calls with the same calling and called number should be detectable by the originating service provider, terminating service provider, and STI-CPS. Therefore, it is recommended that the originating service provider, terminating service provider, and STI-CPS analyze traffic to detect this attack vector and take preventative actions. It is also recommended that STI-CPSs retain PASSporT(s) for as short a time as practical to make this attack vector more difficult to exploit. IETF RFC 8816 section 7.4 [Ref 102] describes this attack vector and mitigation techniques in more detail."

Verizon's 1st security concern has been addressed

- PASSporTs (as defined in RFC 8225) have minimal replay attack prevention. The combination of calling number, called number, and approximate timestamp are all that bind a PASSporT to a call. An attacker with timely access to a PASSporT can perform a replay attack. This is not specific to Out-of-Band SHAKEN.
- Out-of-Band SHAKEN potentially offers an additional attack surface that can be used to perform replay attacks.
- Due to the number of conditions that must be met, the attacker will likely need to originate a large volume of calls to successfully perform a single replay attack. The large volume of calls with the same calling and called number should be detectable by the originating service provider, terminating service provider, and STI-CPS. Therefore, it is recommended that the originating service provider, terminating service provider, and STI-CPS analyze traffic to detect this attack vector and take preventative actions.
- It is also recommended that STI-CPSs retain PASSporT(s) for as short a time as practical to make this attack vector more difficult to exploit.
- IETF RFC 8816 section 7.4 describes this attack vector and mitigation techniques in more detail

Verizon's 2nd security concern has been addressed

- Requires the attacker to possess the private key of a valid SHAKEN certificate
- An attacker with the private key of a valid SHAKEN certificate could spoof a call from any calling number to any called number and create a valid SHAKEN PASSporT with attestation level A
- Requires the attacker to make a large volume of retrieve requests for the same calling and called number to the STI-CPS
- The large volume of requests is easy for the STI-CPS to identify

The Commission should change 47 CFR 64.6303

47 CFR 64.6303 Caller ID authentication in non-IP networks:

"(a) Except as provided in §§ 64.6304 and 64.6306, not later than June 30, 2021, a voice service provider shall either:

(1) Upgrade its entire network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework as required in § 64.6301 throughout its network; or

(2) ~~Maintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop~~ Implement a non-internet Protocol caller identification authentication solution~~, or actively testing such a solution~~.

(b) Except as provided in § 64.6304, not later than June 30, 2023, a gateway provider shall either:

(1) Upgrade its entire network to allow for the processing and carrying of SIP calls and fully implement the STIR/SHAKEN framework as required in § 64.6302(c) throughout its network; or

(2) ~~Maintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop~~ Implement a non-internet Protocol caller identification authentication solution~~, or actively testing such a solution~~."