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

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

# COMMENTS OF TRANSACTION NETWORK SERVICES, INC.

Lavinia Kennedy
James Tyrrell
Paul Florack
TRANSACTION NETWORK SERVICES, INC.
10740 Parkridge Blvd.
Suite 100
Reston, VA 20191
(703) 453-8300
lkennedy@tnsi.com
jtyrrell@tnsi.com
pflorack@tnsi.com

Steven A. Augustino
KELLEY DRYE & WARREN LLP
3050 K Street, NW
Suite 400
Washington, D.C. 20007
(202) 342-8612
saugustino@kelleydrye.com

*Its Counsel*

July 24, 2019

# SUMMARY

Transaction Network Services, Inc. ("TNS"), by its attorneys, hereby provides comments in response to the Commission's Third Further Notice of Proposed Rulemaking ("*Third FNPRM*") in the above-captioned proceeding.

TNS supports the Commission's efforts to promote the implementation of the SHAKEN/STIR framework and, ultimately, to reduce unlawful robocalls. Through a combination of robust analytics inputs and greater trust and authentication in the telecommunications network, TNS believes that the industry can make a material impact on the problem of illegal and unwanted calls. However, TNS urges caution in implementing the specific proposals made in the *Third FNPRM.* It is premature for the Commission to authorize call blocking based solely on the failure of call authentication or the lack of an authentication signature alone. There are many reasons why such authentication might fail at this early state of SHAKEN/STIR deployment, and TNS urges the Commission not to sanction blocking that exceeds the capabilities and role of the current SHAKEN/STIR framework. Instead, TNS recommends that the Commission clarify that it is permissible for voice service providers to consider the SHAKEN/STIR information as part of a broader call blocking program backed by reasonable analytics. By recognizing the limits of the SHAKEN/STIR framework and using analytics to supplement that information, the Commission stands the best chance of reducing unlawful calls and restoring trust in voice communications.

TNS urges the Commission to clarify that any safe harbor it identifies for voice service providers also extends to the call analytics provider that partners with the provider to address unwanted calls.

In addition, TNS believes the Commission is in the best position to assist the industry in identifying a Critical Calls List that should not be blocked by an analytics-based system. Commission involvement in identifying critical calls and/or compiling such lists will best serve the goals of consistency and certainty for the critical calling community. If the Commission fails to validate or oversee a Critical Calls List, then the Commission should provide a safe harbor for voice service providers (and their partners) who reasonably attempt to identify such calls.

Finally, TNS addresses several issues relating to the deployment of SHAKEN/STIR. TNS believes that the Commission can encourage broad deployment of the SHAKEN/STIR framework, allow for broader use of analytics, and promote interim solutions such as Out-of-Band STIR.

## TABLE OF CONTENTS

**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, DC**

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

## COMMENTS OF TRANSACTION NETWORK SERVICES, INC.

Transaction Network Services, Inc. ("TNS"), by its attorneys, hereby provides comments in response to the Commission's Third Further Notice of Proposed Rulemaking ("*Third FNPRM*") in the above-captioned proceeding.[1]

## I. INTRODUCTION

TNS provides global, dedicated real-time data communication networks enabling industry participants to simply and securely interact and transact with other businesses, while connecting to the data and applications they need. By combining innovation, advanced technology, experience and service excellence, TNS has delivered managed data communications solutions to service providers and enterprises on a global scale since 1991. Its Wholesale Division offers a portfolio of mobile network, identity, discovery and routing solutions to enable the reliable delivery of communications world-wide.

[1] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59 and WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51 (June 7, 2019) ("*Third FNPRM*").

TNS's services include highly inter-connected inter-carrier signaling and call routing services provided to the smallest to largest voice service providers, which provides a basis for the TNS Call Guardian service, a robocall detection solution implemented by four of the six largest wireless carriers in the United States. Call Guardian utilizes information from over 1 billion signaling transactions per day traversing the TNS signaling network in order to differentiate legitimate users of communications services from illegal and unwanted calls. Call Guardian integrates this data with numerous other industry data sources, SHAKEN/STIR parameters, and crowd sourced data, to analyze calls in real-time and determine a Telephone Number Reputation score and category that is used by its voice service provider partners. Call Guardian is a dynamic scoring system that takes into account historical reputation information and "real-time intelligence" to constantly re-assess calls, spot suspicious behavior and to keep pace with evolving tactics used by bad actors seeking to perpetrate scams and other malicious behavior. Earlier this year, TNS, in partnership with Metaswitch, launched the Call Guardian Authentication Hub which is a hosted/managed implementation of the SHAKEN/STIR framework that integrates seamlessly with analytics.

TNS is a strong supporter of efforts to identify and reduce unwanted and illegal robocalls. TNS data shows that neighbor spoofing and toll-free spoofing are significant problems in the industry. Since TNS debuted neighbor spoofing tracking in mid-2018, it has seen an increase in the tactic. Twenty-four percent (24%) of all negatively-scored calls are scam/fraud calls that employ neighbor spoofing.[2] Meanwhile, legitimate customer care numbers (predominantly toll-free numbers) are being spoofed with increasing regularity, to the point that

[2] TNS, 2019 Robocall Investigation Report, at 5, March 2019 (filed May 15, 2019 in CG Docket No. 17-59) (https://www.fcc.gov/ecfs/filing/10515248878426).

more than two-thirds of calls displaying a toll-free number are scored as nuisance or high-risk by TNS.[3] Not surprisingly, scam artists are adapting their tactics, with TNS observing an increase in the use of "snowshoe spamming," an effort to send spam over multiple telephone numbers in low-enough volume on each number so as to avoid detection by most call filters.[4] Because of the nature and complexity of unlawful calling, many complementary solutions will be necessary.

## II. THE COMMISSION SHOULD AUTHORIZE USE OF CALL AUTHENTICATION AS A FACTOR IN CALL BLOCKING PROGRAMS

The *Third FNPRM* asks whether the Commission should adopt a safe harbor for voice service providers that choose to block calls (a) that fail Caller ID authentication under the SHAKEN/STIR framework or (b) that originate on the network of a voice service provider participating in SHAKEN/STIR but which are unsigned.[5] For the reasons explained below, TNS does not support blocking based *solely* on the failure of authentication or lack of a signed certificate in these circumstances. Such a blanket blocking rule places too much reliance on the SHAKEN/STIR framework, which is not designed to carry the weight such a rule would impose. Instead, TNS supports permitting voice service providers to utilize SHAKEN/STIR information *along with reasonable analytics* in call blocking programs. TNS would support a safe harbor that enables the blocking of some calls identified in the *Third FNPRM*, if analytics also were employed and the call was identified as likely unlawful.

[3] *Id.* Not all negatively scored calls are illegal. A negative score can represent calls on a range from a mere nuisance to a dangerous scam call. TNS's carrier partners ultimately determine the labeling to apply to negative scored calls and whether to block high-risk negative calls.

[4] *Id.* at 19.

[5] *Third FNPRM* at ¶¶ 51, 54.

### A. SHAKEN/STIR is Designed to Combat Robocalls by Making Spoofing More Difficult and by Identifying the Source of Calls, Not by Determining the Lawful or Unlawful Intent of the Caller

TNS supports the efforts of the communications industry to implement the call authentication framework (known as SHAKEN/STIR) in order to authenticate the telephone number used by callers. STIR and SHAKEN use digital certificates, based on common public key cryptography techniques, to ensure the calling number of a telephone call is secure.[6] When fully deployed, SHAKEN/STIR will authenticate the Caller ID at the origination point of the call, then validate this Caller ID at the termination point. This framework is designed to identify Caller ID spoofing, a common technique used by unlawful robocallers.

However, it is just as important to recognize the limitations of SHAKEN/STIR. As many commentators noted at the FCC's SHAKEN/STIR Robocall Summit in July 2019, the framework is not a "silver bullet" to prevent robocalls.[7] The NANC Call Authentication Trust Anchor Working Group stated that, SHAKEN/STIR "allows communications service providers to attest the legitimacy of a calling party's number."[8] The Working Group cautioned, however, that, "Although SHAKEN provides a mechanism for all authentication, this system does not establish call validation treatment applications (e.g., call blocking or certified identity)," even

[6] *See generally, Call Authentication Trust Anchor*, Notice of Inquiry, WC Docket No. 17-97, FCC 17-89 (July 14, 2017) (describing the SHAKEN/STIR framework).

[7] *See, Chairman Pai Announces Agenda for SHAKEN/STIR Robocall Summit*, Public Notice, DA 19-635 (rel. July 9, 2019). The video for the Summit is available on the Commission's page at: https://www.fcc.gov/SHAKENSTIRSummit.

[8] North American Numbering Council, Call Authentication Trust Anchor Working Group, *Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR*, at 4 (2018), available at http://nanc-chair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf.

though development of such enhancements is the "next logical step."[9] Thus, the fact that a number is authenticated, by itself, does not determine the lawfulness of the call being made.

This is true because while SHAKEN/STIR can attest to the authentication of the *number*, that doesn't answer the question as to the validity of the call itself. A validated number can still be used to send unlawful calls, for example in the "snowshoe spamming" strategy that TNS's Call Guardian has detected. In snowshoe spamming, a bad actor makes calls from multiple, valid telephone numbers, generally at a volume designed to avoid detection on any specific number. Instead, the malicious calls are spread across a wide enough set of numbers that they either remain undetected or avoid detection long enough to perpetrate the scam. If successful, the calls might all be "valid" and could all be attested in a SHAKEN/STIR environment. The bad actor, however, hopes to be nimble enough to use and abandon numbers before the scam is detected.

SHAKEN/STIR alone won't detect such malicious calls, but with reasonable analytics, the scam could be detected through a multi-faceted reputation analysis.

### B. Even if SHAKEN/STIR Could Be Enhanced to Identify Illegal Calls, at this Stage in its Deployment the Framework is not Ready to Carry That Burden.

The NANC CATA Working Group recognized that the "next logical step" may be service provider- or third-party-supplied enhancements that set treatment conditions based on SHAKEN/STIR results.[10] But the framework still is at an early stage of its deployment. The

[9] *Id.* at 5. The Report further states the expectation that "these applications will extend the greater STI ecosystem with either enhanced voice service provider services or third-party applications offered as enhancements to traditional telephone services." *Id.*

[10] *Id.* at 5.

STI-Governance Authority has been established, and a Policy Administrator has been selected, but initial implementation is targeted for December 2019. Moreover, so far, predominantly Tier 1 carriers have announced definitive plans to deploy SHAKEN/STIR. Those carriers that have announced such plans account for less than 50% of total traffic,[11] whereas 87% of the negative traffic is coming from numbering resources assigned to entities *outside* the top tier of service providers.[12] SHAKEN/STIR is unlikely to be deployed quickly enough to address the most problematic traffic.

TNS believes the Commission should allow SHAKEN/STIR to be deployed more fully before assessing whether the framework alone is a sufficiently reliable proxy for identifying certain unlawful calls. In the *Third FNPRM*, the Commission posits that a call might fail authentication if the attestation header "has been maliciously altered or inserted."[13] TNS does not see how voice service providers will be able to consistently detect an attestation that has been altered or inserted, much less the source or intent of that change. Moreover, especially at the early stages of deployment, it is possible that the attestation may fail for wholly unrelated reasons, and it would be difficult, if not impossible, to distinguish the cause of a failure using only the SHAKEN/STIR parameters.

Similarly, the fact that a voice service provider has failed to update a signing certificate or the signing certificate has expired should not be viewed as dispositive at this stage of deployment. These conditions could occur for a variety of reasons at the outset – including

[11] *2019 Robocall Report* at 27.

[12] *2019 Robocall Report* at 12.

[13] *Third FNPRM* at ¶ 51.

mere oversight or lack of sufficient methods and procedures. Penalizing such service providers – and potentially harming legitimate callers – by blocking calls is a remedy that doesn't fit the failure at this time.

Further, the failure to insert a signature on a particular call – as posited in paragraph 54 of the *Third FNPRM* – could also result from oversight or inadequate experience with the SHAKEN/STIR framework. This condition, consequently, is not suitable for categorical treatment decisions by terminating carriers.

### C. SHAKEN/STIR Information Can Be a Suitable Input to a Robust Call Blocking Program, and a Safe Harbor for Analytics-Backed Blocking Using Some Conditions Could Be Justified

Instead of permitting blocking based solely on a SHAKEN/STIR condition, TNS recommends that the Commission explicitly allow service providers to include SHAKEN/STIR information in their analytics-backed blocking programs. SHAKEN/STIR can assist in detection and prevention, even where, by itself, the framework is not designed for that particular task. For example, while a failed authentication, by itself, may not demonstrate whether a call should be blocked, that fact could act as a heightened risk factor that, when combined with analytics and crowd-source feedback could indicate that a call poses a substantial risk to consumers. A reasonable analytics provider, therefore, might take SHAKEN/STIR authentication information (or the lack thereof) as a factor in assessing the call. To avoid any doubt, the Commission should clarify in this proceeding that such analytics-backed determinations are permissible.

Such a finding responds to the Commission's questions in the *Third FNPRM* about how SHAKEN/STIR-based analytics might be used.[14] TNS agrees that SHAKEN/STIR's

[14] *Third FNPRM* at ¶ 62.

ability to provide information regarding the source of calls will be a significant contribution to the quality of analytics. SHAKEN/STIR information could support (or refute) information otherwise available regarding a call, thereby helping to improve the predictive nature of the analytics result. The Commission can encourage the use of this information by removing any doubt that analytics providers can use any SHAKEN/STIR-based information as an input into their analysis.

Further, TNS could support a safe harbor, when the SHAKEN/STIR condition also is backed by analytics information suggesting that the call is likely unlawful. TNS believes that at least two SHAKEN/STIR framework indicators might be suitable as inputs into a safe harbor at this time. First, clear evidence of an altered authentication would be such a condition. Second, the repeated failure to authenticate a particular number – by a voice service provider that is known to have implemented SHAKEN/STIR – could support blocking if other analytics-backed indicia indicate the call is suspect.[15] The Commission, therefore could identify these situations as suitable for a call blocking safe harbor when the blocking also is supported by analytics information.

## III. ANY SAFE HARBOR SHOULD PROTECT A VOICE SERVICE PROVIDER AND ITS PARTNERS THAT CONTRIBUTE TO THE DECISION TO BLOCK A CALL OR THAT ASSIST IN ITS IMPLEMENTATION

The Commission concludes that a safe harbor for certain types of call blocking will substantially reduce voice service provider costs while increasing consumer benefit from not receiving unlawful calls. In particular, the Commission tentatively concludes that a safe harbor

[15] Because a single failure to authenticate a number could result from an error or oversight, TNS believes this safe harbor should rely upon evidence that the condition is repeated or persistent, not a one-time occurrence.

will facilitate implementation of call blocking by providing carriers with more certainty regarding their actions.[16] As noted above, TNS suggests a modified safe harbor that differs from the Commission's proposal primarily in that any safe harbor should incorporate reasonable analytics in the blocking decision.

Beyond the difference in application, however, TNS supports the Commission's conclusion that a safe harbor provides benefits that exceed its costs. In particular, as the Commission notes, a safe harbor will provide voice service providers with greater certainty, to the extent, for example, they are protected from claims that the blocking was implemented erroneously or harmed a particular caller. Analytics will be a dynamic endeavor, and although TNS has confidence in the accuracy of its scoring methodology, the possibility of challenges might discourage service providers from implementing blocking decisions based on the analytics. A safe harbor will provide voice service providers with greater certainty, and thus encourage adoption of reasonable call blocking programs to reduce unlawful robocalls.

The benefits of such a safe harbor could be undermined, however, if the safe harbor does not extend to the voice service provider's vendors as well. If a safe harbor protected the voice service provider, but allowed a disgruntled caller to pursue claims against the underlying analytics provider or against a vendor that provided a call blocking solution to the service provider, the benefit of a safe harbor could be lost. Under these circumstances, vendors may be reluctant to provide innovative solutions within the scope of the Commission's parameters, simply because they could face liability if they were to do so (even if the voice service provider could not). Therefore, TNS submits that the Commission should clarify that any

[16] *Third FNPRM* at ¶ 59.

safe harbor adopted in this proceeding protects not only the voice service provider but also its vendors and suppliers that assisted with the blocking.

## IV. THE COMMISSION IS IN THE BEST POSITION TO OVERSEE A "CRITICAL CALLS LIST" OF NUMBERS THAT PROVIDERS MAY NOT BLOCK

The *Third FNPRM* states that "certain emergency calls must never be blocked."[17] The *Third FNPRM* asks a series of questions concerning whether to require voice service providers to maintain a "Critical Calls List" of numbers they may not block, what numbers should be on such a list and how such numbers could be compiled, maintained, and safe-guarded from those making illegal calls.[18]

The Commission's questions raise legitimate questions about the mechanics of maintaining such a list. To its credit, the *Third FNPRM* notes TNS's concern (expressed in 2017) that Commission assistance in "gathering the numbers of emergency and other important services" could be instrumental to the creation of a Critical Calls List.[19] TNS believes that, if a Critical Calls List, is to be required, a single-uniform list is the best way to achieve that goal. The Commission already oversees a number of similar databases, which can serve as a suitable model for a Critical Calls List.

First, the Commission is in a better position than the industry to identify services and numbers that may not be blocked. Public Safety Answering Points (PSAPs) are much more likely to disclose critical and sensitive information to the Commission than they are to multiple

[17] *Third FNPRM* at ¶ 63.

[18] *Id.* at ¶¶ 63-68.

[19] *Third FNPRM* at ¶ 65 (quoting comments from TNS, filed July 3, 2017, at 20).

service providers (or their vendors) that seek to compile such lists. Moreover, the Commission may do so more efficiently, as a PSAP would have only one entity to disclose the information to (the Commission or the entity selected to run a database), rather than determining the dozens or perhaps hundreds of other entities to whom such information should be disclosed.

The Commission also is better suited to make the policy judgment as to which entities are eligible for inclusion in a Critical Calls List. Already, the FCC's *Declaratory Ruling* is subject to a Petition for Reconsideration from the alarm industry, arguing that alarm calls are "emergency calls" that should not be blocked.[20] As the Commission notes, others, including but certainly not limited to schools, doctors, and local governments, may lay claim to "critical call" status, as might providers of fraud alerts, weather alerts, safety recalls and perhaps any number of additional purported "critical" callers.[21] It is not desirable to ask voice service providers (or their vendors) to make judgments as to which of these claimants may be worthy, nor is it reasonable to ask voice service providers to determine which entities fall within the categories the Commission may identify for "critical call" status. Instead, if a Critical Call List is to be maintained, the Commission should oversee the database.

TNS notes that the Commission has already begun a substantially similar endeavor involving PSAPs. Pursuant to the "Middle Class Tax Relief and Job Creation Act of 2012," the Commission was required to establish a Do-Not-Call registry for numbers used by

[20] Petition for Clarification or Reconsideration by the Alarm Industry Communications Committee, CG Docket No. 17-59, WC Docket No. 17-97 (filed July 8, 2019).

[21] *Third FNPRM* at ¶ 66.

PSAPs and prohibiting the use of automatic dialing equipment to call these numbers.[22] The Commission established a PSAP Do-Not-Call Registry and adopted operational rules for the registry in 2012. Importantly, the Registry already contains rules for (a) identifying the telephone numbers that may be included in a registry, (b) registering such numbers by eligible PSAPs, (c) safeguarding such numbers from unlawful disclosure and (d) providing access to the registry by appropriate entities.[23] Although the PSAP Registry has not become operational, the work done by the Commission to establish the registry could be adapted to establish a Critical Calls List. In particular, the Commission could identify the numbers that could be included in the Critical Calls List, establish procedures for the registration of such numbers and control access to the List to appropriate entities.

TNS submits that the Commission should not rely upon voice service providers or their vendors to implement such lists. If the Commission were to require voice service providers to maintain Critical Call Lists, there would be literally dozens, if not hundreds of such lists, and the risk of unlawful disclosure would increase substantially. The risk that a Critical Call List could be abused by unscrupulous callers in order to subvert call blocking mechanisms would be unacceptable. An unscrupulous actor would need only to find the least secure or least vigilant voice service provider in order to gain potentially invaluable information to perpetrate malicious acts.

If the Commission fails to validate or compile a Critical Calls List, then the Commission should provide a safe harbor for voice service providers (and their partners) who

[22] *Implementation of the Middle Class Tax Relief and Job Creation Act of 2012*, Report and Order, FCC 12-129 (Oct. 17, 2012).

[23] *Id.*; *see* 47 C.F.R. § 64.1202.

reasonably attempt to identify such calls. However, a Commission-supervised list is preferable to such an alternative.

## V. OTHER ISSUES

### A. The Commission Should Continue to Allow Voice Service Providers Discretion in Determining the Appropriate Methodology and Processes for Identifying Harmful Calls

At paragraph 58 of the *Third FNPRM*, the Commission asks whether it should require any particular protections to ensure that wanted calls are not blocked. TNS recommends that the Commission not mandate any such mechanisms at this time.

Just as the Commission showed appropriate caution with respect to call blocking rules in the *Declaratory Ruling* portion of the June 7 Order, so should it refrain from interjecting itself into the methodology or procedures used by voice service providers or their vendors. As the Commission noted in the *Declaratory Ruling*, "rigid blocking rules" can be counter-productive and "could impede the ability of voice service providers to develop dynamic blocking schemes that evolve with calling patterns."[24] Indeed, TNS regularly sees changes in scam artists' tactics, and anticipates that with SHAKEN/STIR implementation, scammers will seek to evade the new protections through modified tactics. The Commission should allow voice service providers and their analytics vendors the flexibility to modify their methodologies to keep up with the changing nature of the threats.

The same concerns are true for mechanisms for callers to contest the reputation score of a particular call. Voice service providers have a sufficient incentive to ensure that their

[24] *Third FNPRM* at ¶ 34 (also noting that "a diversity of approaches would create a more challenging operating environment for illegal robocallers." (quoting USTelecom Comments)).

customers receive the calls that they want to receive, and thus will be sensitive to assertions by customers that desired calls are erroneously blocked. TNS's crowd-sourced feedback, however, indicates that current procedures and call analytics are highly accurate: consumers report a false positive on only 0.01% percent of high and medium risk calls labeled by TNS. Indeed, the ability of consumers to opt-out of any blocking should prove an adequate remedy if consumers don't find the blocking accurate enough or find that legitimate calls are being blocked.[25]

Further, TNS and other providers have in place procedures for legitimate callers to provide additional information about their calls, in order to improve the accuracy of the analytics results. The record does not reflect any specific experiences showing that these procedures are deficient or not capable of addressing the concerns of legitimate callers. Unless there is evidence of a failure, the Commission should not insert itself into these processes.

### B. Accelerating the Deployment of SHAKEN/STIR

In paragraphs 71 through 82 of the *Third FNPRM*, the Commission asks a series of questions relating to whether, and if so, how it should mandate the implementation of the SHAKEN/STIR Caller ID authentication framework. TNS supports the broad deployment of Caller ID authentication technologies, and supports the Commission's goal of accelerating the deployment of a full SHAKEN/STIR solution. As TNS noted in its 2019 Robocall Report, 87% of high-risk calls originate using numbering resources outside those of the top 6 carriers.[26] In order for SHAKEN/STIR to have a significant impact, its deployment must expand beyond the

[25] *Id.* (finding that "to the extent certain callers claim that consumers do indeed want to receive calls from them, we believe the ability for consumers to opt out of call-blocking programs adequately addresses such concerns.").

[26] *2019 Robocall Report* at 12.

largest carriers. Indeed, the full benefits of SHAKEN/STIR cannot be achieved until it is nearly ubiquitously deployed.

There are a number of technical and financial impediments to full implementation of SHAKEN/STIR, which will require flexibility by the Commission to overcome. TNS therefore supports measured actions by the Commission to accelerate the deployment of the technology.

Where IP networking is already in place, and where sufficient IP interconnection arrangements are established, it appears that SHAKEN/STIR can be deployed rather quickly. TNS would support a mandate to deploy SHAKEN/STIR by a date-certain for any network with sufficient IP networking in place. Any mandate should provide sufficient time to implement the necessary capabilities while setting deployment as quickly as possible.

Where the necessary IP networking elements are not in place, it appears that near-term implementation is difficult to achieve. For these networks, the Commission should focus on promoting the deployment of interim solutions. For example, TNS has developed a Call Authentication Hub that enables Tier 2 and Tier 3 carriers to deploy SHAKEN/STIR capabilities, and TNS also provides a pre-SHAKEN/STIR solution for TDM carriers using out-of-band signaling.[27] These solutions (and other industry alternatives) could assist smaller carriers and providers using non-IP-based service arrangements to deploy interim capabilities quickly and to move toward the path of full SHAKEN/STIR deployment. Solutions such as Out-of-Band STIR also show promise (as discussed below) and could provide solutions for the limitations presented

[27] *See* Letter from Michael R. McCarthy, TNS, to Marlene H. Dortch, FCC, at 1, CG Docket No. 17-59 and WC Docket No. 17-97, filed June 17, 2019 (*ex parte Notice of Transaction Network Services)* (describing the benefits of TNS's interim solution).

by non-IP networks. These interim solutions, along with analytics-based identification of illegal and unwanted calling, can provide benefits even before deployment of SHAKEN/STIR is feasible.

### C. Providing Benefits for Calls Made on Legacy Network Technologies

Not all calls originate on IP networks. For the foreseeable future, TDM-based networks will continue to serve a role in the U.S. telecommunications landscape. TNS welcomes the Commission's focus on encouraging Caller ID authentication for carriers that maintain at least some portion of their network on legacy technology.[28]

Relative to legacy network support for call authentication, there are options available for those networks to address illegal and unwanted calling. First and foremost, analytics solutions support identification of such calls and are a good bridge to full authentication. Voice service providers can take advantage of analytics-based call labeling or call blocking technologies, even where SHAKEN/STIR deployment is not feasible. These technologies will provide their customers with tools to combat unlawful robocalls, and should be encouraged.

Secondly, TNS has developed out of band STIR functionality for various use cases and the technology shows promise. The technology is called out of band STIR because the authentication of the call is communicated separately from the call signaling information. Call authentication information is reported by Call Guardian to the central STIR database and the central database reports it to the terminating carrier. This contrasts with the traditional SHAKEN/STIR implementation, where authentication of the call is carried inside the call

[28] *Third FNPRM* at ¶ 80.

signaling itself vis the SHAKEN PASSporT Identity header. Benefits of the out of band approach include improved accuracy of the Call Guardian reputation scores and "authentication" of calls even without full SHAKEN/STIR implementation. Moreover, out of band STIR could be applied to non-SIP based calls.

The industry is continuing to study out of band STIR and are working to address the details of such deployments. TNS expects progress on these issues to proceed without the need for active Commission involvement. Legacy networks will be incented to deploy these interim solutions as IP networks are protected.

### D. Voice Service Providers Should Be Allowed to Experiment to Develop the Most Beneficial Display Framework for their Consumers

TNS does not support a Commission-mandated "uniform display" for the delivery of SHAKEN/STIR calls.[29] The industry is still experimenting with display information and display formats, and there is much still to be learned regarding what information is meaningful to consumers.

As TNS explained in a recent meeting with FCC personnel,[30] TNS, through its wholly owned subsidiary, Cequint, recently conducted a User Study of display options for the SHAKEN/STIR framework. Key findings of the study were that:

- Telephone number validation with STIR/SHAKEN does not drastically change consumers' behavior on whether they answer incoming calls;

[29] *Third FNPRM* at ¶ 80.

[30] *Ex parte Notice of Transaction Network Services*, June 17, 2019.

- 8 out of 10 people will not answer a call from an unknown number even when the telephone number has been validated by STIR/SHAKEN; and
- consumers are equally likely to block an incoming call that has been validated by STIR/SHAKEN compared to a call that has not been validated.[31]

One of the key lessons from the study was that consumers found that displaying the identity of the caller and the purpose of the call were much more important to their decision whether to answer the call. When only the telephone number is displayed, 79% of wanted calls are not likely to be answered, but when more information is provided, 71% of consumers are likely to answer. Said differently, when only the telephone number is displayed, the answer rate for a wanted call is only 21%, but when the telephone number plus other information are provided, the answer rate for the same call increases to 71%.

Thus, the ability to display the (verified) identity of the caller and the purpose of the call were key features that consumers desired. By contrast, telephone number validation was less meaningful to consumer behavior, even as analytics to identify and block "bad" calls remains a key goal of voice service providers today. This suggests that, at a minimum, further education is necessary for consumers to identify that a telephone number has been validated under SHAKEN/STIR and to understand the significance of such validation. It also presents a challenge for voice service providers delivering calls under the SHAKEN/STIR framework, as they must determine how best to convey caller information and/or purpose information to consumers on a variety of devices.

[31] The results of this study were also presented to the ATIS IP-NNI Task Force on May 1, 2019. That presentation is attached to these comments as Exhibit 1.

### E. The Commission Should Not Adopt a Formal Mechanism for Measuring the Effectiveness of Anti-Robocall Solutions

TNS does not support calls for "the Commission [to] create a mechanism to provide information to consumers about the effectiveness of various voice service providers' robocall solutions."[32] TNS does not believe the Commission needs to require such reporting to consumers. Analytics providers rely on proprietary algorithms to determine not only how a call is labeled but also false positive rates and accuracy. The methodology used can differ among providers which makes it difficult to define the "effectiveness" of the robocall solutions. Any attempt to establish a measurement for all providers to use is likely to reduce to a "lowest common denominator" that potentially stifles the innovation and nimbleness needed to track illegal robocallers' varying tactics. Moreover, consumers already have the most effective means to object to call blocking programs that are not sufficiently effective: they may opt out of a voice service providers' program and utilize one of hundreds of available third-party applications designed to combat unwanted robocalls.

## VI. CONCLUSION

TNS supports the Commission's efforts to promote the implementation of the SHAKEN/STIR framework and, ultimately, to reduce unlawful robocalls. Through a combination of robust analytics inputs and greater trust and authentication in the telecommunications network, TNS believes that the industry can make a material impact on the problem. TNS urges the Commission not to sanction blocking that exceeds the capabilities and role of the SHAKEN/STIR framework alone, and instead to authorize voice service providers to

[32] *Third FNPRM* at ¶ 83.

consider the SHAKEN/STIR information as part of a broader call blocking program backed by reasonable analytics. By recognizing the limits of the SHAKEN/STIR framework and allowing analytics to supplement that information, the Commission stands the best chance of reducing unlawful calls and restoring trust in voice communications.

TNS urges the Commission to sanction use of SHAKEN/STIR authentication information as described above, to establish a reasonable safe harbor for voice service providers and their vendors that act to address unwanted calls, and to assist the industry in identifying critical calls to be protected.

Respectfully submitted,

Steven A. Augustino
KELLEY DRYE & WARREN LLP
3050 K Street, NW
Suite 400
Washington, D.C. 20007
(202) 342-8612
saugustino@kelleydrye.com

*Its Counsel*

Lavinia Kennedy
James Tyrrell
Paul Florack
TRANSACTION NETWORK SERVICES, INC.
10740 Parkridge Blvd.
Suite 100
Reston, VA 20191
(703) 453-8300
lkennedy@tnsi.com
jtyrrell@tnsi.com
pflorack@tnsi.com

July 24, 2019