July 19, 2019

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Comments on DECLARATORY RULING AND THIRD FURTHER NOTICE OF PROPOSED RULEMAKING in the matter of:

Advanced Methods to Target and Eliminate Unlawful Robocalls (CG Docket No. 17-59)
Call Authentication Trust Anchor (WC Docket No. 17-89)

Dear Ms. Dortch:

TransNexus files these comments in response to proposed rulemaking in the matter of blocking unwanted robocalls.

TransNexus provides software products to help telecommunications service providers and enterprises manage and protect their telecommunications networks. These products include features to block robocalls and perform SHAKEN/STIR authentication and verification of caller ID. The software is live in production networks of our customers.

We use our experience in developing, testing, and deploying this software with our customers as the basis for our commentary on the proposed rulemaking, especially regarding items 51–58 and 80 in the Third Further Notice.

51. First, we propose a safe harbor for voice service providers that choose to block calls (or a subset of calls) that fail Caller ID authentication under the SHAKEN/STIR framework… we would expect the vast majority of calls blocked in such circumstances to be illegitimate and call-blocking programs targeting such calls to be deserving of safe harbor. We seek comment on this view.

TransNexus comment: We agree with establishing a safe harbor for blocking calls that fail authentication. However, we expect that most providers will not want to block calls by default. Instead, we find that providers would rather give their customers the choice.

For example, a hospital or health clinic will generally answer all calls no matter what. They do not want to miss calls that might be very important.

Many individual consumers, however, have no such concerns and would be happy to have suspected robocalls blocked.

We get a lot of questions from voice service providers asking about call blocking policies. We believe service providers should not make these decisions but should leave it to their customers. This approach has been well received. We designed our software to support this.

52. Are there other instances where authentication would fail? […] As SHAKEN/STIR becomes more widespread, will failed authentication be a good proxy for illegal calls? […] How should we address false positives?

TransNexus comments: Yes, there are other instances where authentication would fail. To avoid confusion and improve policy administration, we designed our software with separate policy actions for different types of failure:

- **Invalid Identity Header** – The call was signed, but the signature doesn't match the content. This is likely a poor attempt at malicious fraud. We expect most providers would block such calls.
- **Certificate Repository Error** – The call was signed, but the software was unable to fetch the certificate from the Certificate Repository. This is likely a problem with internet connectivity or the CR site. We expect most providers would not block such calls but would want to be alerted so they could investigate.
- **No Identity Header** – The call was not signed. We expect providers will not block unsigned calls by default for quite some time. Obviously, none of our customers are blocking unsigned calls currently.
  We designed our software so that providers can set up different policies for different groups of calls, such as trunk groups or carriers. This way, if an inbound call is unsigned and received from a carrier who signs their calls, such calls could be blocked. If another inbound call is received from a different carrier who does not yet sign their calls, such calls should be accepted.

We feel it is important to provide precise, granular controls so that providers can fine tune their policies to meet their business objectives and customer requirements.

This will also address the concern over false positives. Enterprise customers, especially hospitals and health clinics, have a very low tolerance for false positives. Given a preference, they would choose light blocking, probably only signed calls that fail verification. Many consumers, on the other hand, would much rather block unwanted robocalls than worry about false positives. Providers don't have to decide—let the customer decide. One size does not fit all.

As far as whether failed authentication will become a good proxy for illegal calls, it seems unlikely that people sending unwanted robocalls would bother to attempt to sign a call that would certainly fail verification. It would be a complete waste of time. We expect to see very little of that, if any.

It seems more likely that robocall perpetrators would simply procure inexpensive numbers from providers who will sign their calls. This will not last long, however, as call analytics, i.e., reputation services, will eventually tag that number with a poor reputation. At this point, the robocall perpetrator would abandon that number and get another one.

This illustrates how SHAKEN/STIR will not stop unwanted robocalls all by itself. It becomes truly valuable when combined with other services, such as call analytics/reputation services.

Another possible response of robocall perpetrators would be to focus their robocalls at numbers assigned to rural ILECs and CLECs. These providers generally connect to the Public Switched Telephone Network over SS7 TDM trunks, which are unable to transmit Identity tokens in-band. This will make rural customers prime targets for robocalls. We discuss this further in our response to items 56, 57 and 80, below.

53. We note that call-blocking programs that consider the degree of attestation (whether full, partial, or gateway attestation) for successfully authenticated calls would not fit within the scope of this safe harbor. Further, only calls for which attestation information is available—the originating provider has implemented SHAKEN/STIR and each intermediate provider in the call path accurately passes authentication information to the terminating provider—and that fail authentication would be blocked. Is that striking the appropriate balance?

TransNexus comment: Consistent with our remarks above, we believe that call blocking policy choices should be left to the subscriber customer.

If a subscriber only wants to receive calls signed with either full or partial attestation, then that should be their choice. This would be a rather severe call blocking policy, but no more so than blocking all calls from numbers not on a subscriber's whitelist. And if a subscriber chooses strict call blocking, it would be their fault if they miss wanted calls through overzealous blocking.

Attestation level creates adverse incentives that threaten to undermine the effectiveness of SHAKEN/STIR. If providers find that call completion is greater for calls with full attestation but terrible for calls with partial or gateway attestation, then they have an incentive to sign all calls with full attestation, even in circumstances where it is not warranted. This could undermine consumer trust in SHAKEN/STIR. Therefore, we agree that it makes sense to provide safe harbor for blocking calls without regard to the degree of attestation.

54. Should we create a safe harbor for blocking unsigned calls from particular categories of voice service providers? For example, if a voice service provider is participating in the SHAKEN/STIR framework but fails to sign certain calls, should blocking such calls fall within the safe harbor? Are there any legitimate reasons why a subset of calls should be unsigned?

TransNexus comment: We agree with establishing a safe harbor for blocking unsigned calls from voice service providers who are participating in the SHAKEN/STIR framework. If they're in, they should sign *all calls* that leave their network. Otherwise, unsigned calls could be malicious robocalls that many consumers want to block.

Notice that this requirement would include calls that transit their network but neither originate nor terminate within their network. Interexchange carriers should sign unsigned calls to provide traceback.

Providers may want to perform SHAKEN/STIR functionality on in-network calls too, or they may wish to simply verify calls that never leave their network.

We believe it should be up to the service provider to declare when they are signing calls. Once this declaration has been made, other carriers may then choose to offer to their subscribers the option to block unsigned calls from participating providers. Again, subscribers should be in the driver's seat in determining whether such calls should be blocked.

55. Should safe harbor target those voice service providers that are most likely to facilitate unlawful robocallers? […] Should a safe harbor target those voice service providers that do not appropriately sign calls and do not participate in the Industry Traceback Group? Or should the safe harbor extend only to call blocking for those that do not appropriately sign calls and send hundreds, thousands, or millions of apparently unwanted calls to American consumers? […] should the safe harbor be reserved for voice service providers that provide an incorrect level of attestation?

TransNexus comment: While we understand the reasoning behind this question, targeted safe harbor seems difficult to implement fairly and objectively.

We believe it would be much fairer and more practical to extend a broad safe harbor to blocking unsigned calls, at the request of subscribers, from providers who have declared that they are signing all calls that leave their network.

If a provider assigns incorrect levels of attestation to their calls, then complaints against that provider should be registered and documented with the STI-PA (Policy Administrator). The STI-PA has the authority to revoke the offending provider's certificate. Providers who sign incorrectly risk losing their ability to sign calls.[1]

56. Although we recognize that smaller voice service providers serving rural America will eventually implement the SHAKEN/STIR framework, we are also conscious that they may need more time than their larger peers to transition their networks to Internet Protocol (IP) while also meeting their universal service obligations to deploy voice-capable broadband networks. How can we ensure that any safe harbor does not impose undue costs on eligible

[1] ATIS-1000080. Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management, p. 21, https://www.atis.org/sti-ga/resources/docs/ATIS-1000080.pdf. Retrieved July 11, 2019.

telecommunications carriers participating in the Commission's high-cost program? And how can we ensure any such carve-out does not protect those few voice service providers that actively facilitate unlawful spoofing and robocalling, often from foreign countries?

TransNexus comments: There are several underlying issues to unpack when considering SHAKEN/STIR deployment among smaller rural voice service providers.

First, these providers cannot participate in SHAKEN/STIR as easily as larger providers, even if they install a SIP trunk in their network and SHAKEN/STIR software. Their calls usually transit several interexchange carriers. If any of these segments are not using SIP over TCP/IP, then SHAKEN/STIR will usually fail. These issues are completely outside of the control of the smaller rural service providers.

Second, smaller rural providers face a financial disincentive to switch from their SS7 TDM networks to an IP network. They would lose terminating access fees while incurring the costs of installing a new network.

There is a technical answer to the first problem, called Out-of-Band STIR.[2] It is a technique of transmitting the Identity token from the originating provider to the terminating provider over the internet, outside of the call path. This enables any service provider to participate fully in SHAKEN/STIR regardless of the network readiness of the transit carriers who route their calls. For this reason, we have added Out-of-Band STIR as an option in our software.

The issue with financial disincentives is very real and will affect the rate of SHAKEN/STIR deployment. It will bifurcate the market into the "haves" and the "have nots." However, we feel it is outside of our area of expertise to propose solutions for this issue.

57. Can downstream providers reliably determine on which network a particular unsigned call originated? Are there concerns regarding a call that was initially signed transiting a non-IP network; for example, what is the risk that header information would be lost in transit on a non-IP network? Should we set a date certain for when this type of blocking is permissible?

TransNexus comments: This is a very real concern. There are many reasons why Identity tokens can be lost in transit. SS7 TDM networks is one. But *even SIP networks* over IP have vulnerabilities that can cause SHAKEN/STIR to fail:

- Many of these networks use UDP, which is prone to packet fragmentation and packet loss.
- Many network switches and software are unable to deal with packet fragmentation and packet lost.

[2] STIR Out-of-Band Architecture and Use Cases, tools.ietf.org/html/draft-ietf-stir-oob-05, retrieved July 19, 2019

- Many network switches and software remove the Identity header.

The remedies for these problems require vendors to update their equipment and software that service providers use. Deployment also may require sizeable investments by service providers, which may take several years.

We have found that Identity tokens do not survive transit across SIP networks today, and we have no idea how long it will take to deploy fixes to make the network ready for SHAKEN/STIR.

This is why we added Out-of-Band STIR capabilities to our software. It buys time so that SHAKEN/STIR can work successfully for any service provider today, long before the telephone network is fully capable of supporting it. It enables Identity tokens to be sent from any originating provider to be sent to the terminating provider reliably.[3]

If Out-of-Band STIR becomes widely adopted, then the FCC could set a date for blocking unsigned calls. If SHAKEN/STIR relies solely on in-band transmission of Identity tokens, it will likely take a long time before the network is ready for SHAKEN/STIR.

58. Are there any particular protections we should establish for a safe harbor to ensure that wanted calls are not blocked? We further seek comment on whether to require voice service providers seeking a safe harbor to provide a mechanism for identifying and remedying the blocking of wanted calls. Is such a mechanism necessary? Should we require voice service providers to send an intercept message to blocked callers or return a specific SIP or Integrated Services Digital Network User Part response code when calls are blocked? Are there other approaches that would be more appropriate?

TransNexus comment: Identifying a call as "wanted" is completely subjective. Only the called party can determine that. For any given calling party, some subscribers would identify their calls as wanted while others would say such calls are unwanted. We believe that the *called parties* should have exclusive decision rights over this classification, not the calling parties.

Therefore, we do not think safe harbor should be contingent on identifying calls as wanted or unwanted. If a subscriber does not want calls from a particular calling party, then he or she should be able to block them, and the terminating provider should be covered by safe harbor in doing that.

We offer some observations on SIP signaling that inform our comments on response codes.

Currently, our software blocks a call by returning a *SIP 603 Decline* message. Every piece of SIP network equipment and software we are aware of knows what to do when it

[3] Out-of-Band STIR, transnexus.com/whitepapers/out-of-band-stir/, retrieved July 11, 2019

gets that message. It stops trying to send the call or failing over to another delivery route. It does not explain to the calling party why their call was declined.

There is a proposal under consideration in IETF RFC 8197 to develop a new SIP response code, a *SIP 607 Unwanted* message.[4]

The proposed *SIP 607 Unwanted* differs from the standard *SIP 603 Decline* message in use today in that the 607 indicates that the called party did not want the call because of who the calling party was. The 603 in wide use today is a broader message that does not communicate a reason for rejecting the call.

The intention behind this proposal is to enable the called party to indicate that he or she did not want a call just received. The proposal states that "User feedback may be offered through smartphone apps, APIs or within the context of a SIP-initiated call."

The terminating service provider may offer services to subscribers for future call treatment based upon generation of a *SIP 607 Unwanted* response. For example, they could:

- Blacklist the calling number so future calls from that number would be blocked
- Record the call rejection in a crowd-sourced database for call analytics based upon caller reputation
- Use the event to report to a consumer complaint system.

These call treatments would be more effective when used in conjunction with SHAKEN/STIR to determine whether the caller ID was spoofed.

The SIP 607 proposal does not elaborate on feedback to the calling party that their call was rejected. Simply receiving the SIP 607, however, would inform the called party that the called party does not want their calls.

The SIP 607 proposal has not yet been finalized. Should it become finalized, we will support it in our software.

80. Legacy Networks. As explained earlier, SHAKEN/STIR as developed is intended for IP-based networks, and thus, is less effective for calls that originate, terminate, or transit across TDM networks and does not work at all for calls that exclusively traverse TDM networks. Although the Commission has encouraged carriers to transition to IP networks as soon as possible, we recognize that there are challenges for smaller and rural carriers. We therefore seek comment on how to encourage Caller ID authentication for carriers that maintain some portion of their network on legacy technology. Are there technologies available to enable legacy networks to participate in Caller ID authentication? For example, there is work on "out of band STIR" in the IETF.136 Should we take further steps to promote or require Caller ID authentication on legacy networks? If so, what steps should we take? For

[4] A SIP Response Code for Unwanted Calls, tools.ietf.org/html/rfc8197, retrieved July 10, 2019

example, should we require voice service providers that have implemented the SHAKEN/STIR framework to sign calls entering their network with either partial or gateway attestations?

TransNexus comment: We believe participating carriers should sign unsigned calls entering their network.

There are technologies available to enable legacy networks to participate in caller ID authentication. Many legacy network endpoints could participate in SHAKEN/STIR today by using the following:

- A TDM-to-SIP gateway
- A SHAKEN/STIR software solution that supports Out-of-Band STIR. We have added this option to our software products. Providers using our solutions can send Identity tokens in-band, out-of-band, or both.

With these components, an inbound or outbound call would first be routed to the TDM-to-SIP gateway either for authentication or verification respectively. The gateway would send the call to the SHAKEN/STIR software in a SIP message, where either authentication or verification would be performed as appropriate.

The SHAKEN/STIR software would return a response message back through the gateway to the switch, which would then either originate or terminate the call. For outbound calls, our software would also send an Identity token out-of-band to the terminating service provider so they could verify caller ID using information from the source of the call.

We do not propose this arrangement as a way of extending the longevity of TDM networks. There are plenty of persuasive reasons for service providers to consider making such a move (e.g., obsolescence, lack of spare parts, lack of trained service personnel, lack of support). But there are also substantial financial hurdles to overcome. And the network just isn't close to being ready.

We simply mention this technique as a method to enable these service providers to participate in SHAKEN/STIR sooner rather than later and extend the benefits to all consumers.

+++++

This concludes our remarks on the third further notice of proposed rulemaking.

Respectfully submitted

/s/ Jim Dalton

Chief Executive Officer, TransNexus