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

TNS' COMMENTS ON PUBLIC NOTICE

Since 2015, TNS has maintained a strong focus on aiding our calling provider partners as they seek to restore trust in voice calls. TNS appreciates the opportunity to respond to the FCC's Consumer and Governmental Affairs Bureau's (Commission's) solicitation for input on the progress made in combating illegal and unwanted robocalling. TNS will provide data and other information supporting our assessment of the current and future robocalling landscape.

TNS has gained insights we share within the policy and technical spheres as a function of our work creating the industry-leading analytics server, TNS Call Guardian. Our Call Guardian product analyzes roughly one billion call events across hundreds of carriers every day and bases robocall scoring and categorization provided to our partners on this data. TNS ensures that Call Guardian evolves in response to emerging bad actor trends, such as neighbor spoofing (the use of the same or similar NPA-NXX as the call recipient's number), and perceives the evolution of bad actor calling tactics as a response to the success the industry is seeing in addressing current bad actor methodologies. TNS Call Guardian provides the robocall analytics for Verizon (wireless and wireline), Sprint, and US Cellular, among others.

The Commission has accurately identified the fact that addressing malicious and harassing robocalls requires the multi-pronged approach that so many of us have been engaged in for these past several years.

I. Do-Not-Originate and Calls from Invalid, Unallocated, or Unused Numbers

The Commission provided new permissive rules from the November 2017 Call Blocking Order, which became effective in February 2018, allowing providers to block calls from phone numbers on a Do-Not-Originate (DNO) list and those that purport to be from invalid, unallocated, or unused numbers. [1] TNS has responded by creating an additional level of scoring through which DNO numbers are tracked, and has begun to work with clients as they seek to develop method and policy around a DNO service.

Additionally, TNS ensures that invalid or unallocated numbers are categorized as spoofers. This information is provided to our carrier partners. That said, as we have shared previously, the percentage of problem calls addressed via these rules are quite small, and there is support for the suggestion that suppressing the use of unallocated or invalid numbers in spoofing will encourage the use of assigned numbers, instead. TNS notes that, while the number of telephone numbers identified as spoofers has almost doubled between January and June of 2018, just under 5% of negatively-scored numbers fall into the unallocated or invalid spoofer category.

II. STIR/SHAKEN

TNS stands ready to support implementation of STIR/SHAKEN in 2018 and its continued roll-out in 2019 and beyond. TNS also shares that it is crucial to understand what a full STIR/SHAKEN implementation will and will not be able to provide in terms of protections.

[1] https://docs.fcc.gov/public/attachments/FCC-17-151A1.pdf

STIR/SHAKEN will act as a valuable input to analytics servers, contributing to a determination about how a call should be routed and/or displayed to end users. In addition, TNS supports traceback functionality, which will be aided by STIR/SHAKEN, and has been working with our carrier partners to support these efforts to-date.

Today, it is possible to detect Caller ID spoofing and other malicious and nuisance robocalling behavior based on real-time network data analytics; in other words, the Analytics Server functionality described in the October 2016 FCC Robocall Strike Force report is available now. STIR/SHAKEN and DNO will eventually remove some of the burden borne by the analytics server today, but will not render this crucial analytics component unnecessary. [2] As ATIS, with their understanding of and work on STIR/SHAKEN, has frequently shared in public fora, STIR/SHAKEN is able to attest to the authentication of the calling party telephone number, but is not able to address the question of intent. Bad actors will be able to make malicious calls from numbers that they have been assigned by a provider, and will be able to burn through those numbers, then move on to the use of new numbers in order to avoid detection. The ability to make real-time decisions about a telephone number's reputation based on calling behavior, as provided today by the analytics server role, will continue to provide an essential layer of consumer protection. Additionally, today's analytics server functionality is not dependent on business inputs and participation, as DNO is, nor is it limited to domestic SIP-to-SIP calls, as STIR/SHAKEN is for the foreseeable future. Access to our analytics server is available for all types of Service Providers across all networks, whether VoIP or TDM, via ENUM, SIP, AIN, or RESTful API.

[2] https://www.fcc.gov/file/12311/download

TNS has identified a number of questions related to STIR/SHAKEN's implementation. Some have been addressed, while others remain. Examples include: How secure is the computer storing the private key? How are certificate recipients validated? What happens after call validation? How is the public educated about initiating a traceback? Where will post-call reporting take place? How are tracebacks enforced? Can a private key be intercepted and misused? How are keys revoked? What happens when a number is ported? What's the TTL for a certificate and can it be extended via a hack? How are third parties making legitimate calls on behalf of an enterprise authorized to spoof their caller name and number? What must operators buy and deploy? When will it be available? How much will it cost? How, if at all, do we recover costs of implementing a strategy? What will our liability be if we block a good call? Or authenticate a bad call?

STIR/SHAKEN is indisputably an essential foundational layer to combat spoofing. TNS also shares that it is crucial to understand its limitations and the ongoing need for the real-time analytics layer.

III. FCC/FTC Consumer Complaint Data

The Commission has asked about the use of shared FTC and FCC consumer complaint data. We do find this data useful. TNS takes the complaint files and uses this information alongside crowd-sourced consumer data provided via our Caller Name ID interface through which our Call Guardian data is displayed.

IV. Filtering Criteria

The Commission seeks information about criteria filtering tool providers use in selecting calls for consumers to block or label as illegal or unwanted. In this area, TNS strikes a balance by offering tools both to the carriers to pass on to consumers and to enterprise in order to ensure that they can dispute their characterization by our algorithm and to allow those enterprises to conform to behavior that is less likely to result in negative characterizations of their outbound numbers. Furthermore, TNS has launched publicly-available, industry-leading web sites to allow consumers and enterprises to provide feedback about both calls they have received and their own telephone numbers.

TNS has created a product, TNS Reputation Insights, that allows enterprises access to their number scoring and categorization data. We work closely with enterprises to help those with good intent but little transparency to understand this process of assessment and to adjust behaviors in order to avoid triggering negative reputational scoring. With respect to the implementation of our Call Guardian service with our partners, we defer to their desire to divulge details with respect to thresholds and the choice to block or warn.

V. Trends

TNS shares a few notable trends, using the FCC's requested baseline of January 2018. Between January and June 2018:

- Robocall activity continued to increase over the last six months, with the number of positively rated robocalls growing even faster than negative rated robocalls
- A majority of all outbound calls from toll-free numbers were scored negatively
- One-third of calls from VoIP numbers were negatively-scored
- The volume of negatively-scored VoIP calls was double that of the toll-free calls
- The amount of user-initiated feedback has nearly doubled, indicating that users are more proactively providing feedback, predominantly reporting spam, scam, or telemarketing calls

- As noted earlier, the use of invalid numbers continues to rise, doubling over the past six months, but volume from such numbers continues to be relatively low compared to the rest of the negatively rated calls
- Real time analytics is proving to be effective in identifying spoofed call activity. TNS is identifying tens of thousands of spoofed neighbor calls a day with its latest technology deployment

VI. Enterprises

In addition to trends within the industry that have already been commented on, such as neighbor spoofing, TNS has observed a varied response among enterprises to the mitigation techniques we and others have employed. Largely, among the good actors, though there has been discomfort with this new world in which their calls are being analyzed and characterized, there has been a willingness to adapt methodologies to conform with the analytics tools' definitions of good behavior. As a result, TNS has worked with partners and enterprise allies to develop tools such as Branded Calling, through which a logo and other business information may be displayed. Further, TNS has developed and is in trials with our Reputation Insights product. This solution provides enterprises with a lens into their call centers' practices and allows them to understand what will and will not trigger negative reputational scores. The registration of calling campaigns, for example, will yield positive results, as analytics engines better understand sudden spikes in calling traffic. Specific to enterprises, one commonly observed trend is Enterprises whose main outbound calling numbers are used for multiple purposes tend to get flagged by analytics engines and receive very mixed feedback from consumers. TNS recommends segmenting the use of toll-free numbers for various enterprise purposes. A number used for debt collection, for example, should not be used for other purposes, as consumers will invariably provide negative feedback about the number which will impact other outreach efforts via the same number.

CONCLUSION

TNS again thanks the Commission for the opportunity to take stock of our collective progress over the last several years. In our experience, as others have shared as well, the robocall problem is more complex than it appears on its surface. One has only to attack one aspect of it from either a technical or a policy perspective to learn that it is a Hydra, whereby multiple attendant challenges become clear. For this reason, we support the conclusion that a layered approach will continue to be most effective. This layered approach includes the work being done to implement STIR/SHAKEN, the current analytics server role, policy and structure around DNO, as well as the out-of-band STIR efforts used to support Branded Calling and other initiatives, to restore trust to the calling experience.

Respectfully submitted,

July 20, 2018

Paul Florack