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

In the Matter of	)	
	)	
Call Authentication Trust Anchor	)	**CG Docket No. 17-97**

COMMENTS OF SPRINT CORPORATION

Sprint Corporation ("Sprint") submits these Reply Comments in response to the FCC's Notice of Inquiry in CG Docket No. 17-97. Sprint and other carriers have worked with the Federal Communications Commission ("FCC" or "Commission") to reduce the intrusions into daily life caused by unwanted and often illegal robocalls. Sprint applauds the Federal Communications Commission ("FCC" or "Commission") and Chairman Pai for taking on these issues directly. Sprint supports efforts to build the SHAKEN/STIR call authentication system and will continue to work with the Commission to address the growing problem of unwanted robocalls. Before mandating or encouraging the adoption of new standards, however, the Commission should be aware of the limitations of proposed authentication systems and ensure it adopts a holistic approach to addressing unwanted robocalls.

I. Introduction

Industry has worked diligently with standards organizations to create a system whereby domestic voice telephone calls transmitted in IP format can be authenticated from beginning to end. Call authentication using the SHAKEN/STIR toolset is one input among several that can signal to a terminating carrier or its customer that the incoming call is an illegal or unwanted robocall. Before mandating the use of SHAKEN/STIR—or even encouraging its widespread deployment—the Commission should evaluate how this tool will fit in with the wider effort to

combat unwanted robocalls.

SHAKEN/STIR cannot work as a solely or primarily U.S.-based standard. Sprint's experience is that a large percentage of unwanted robocalls originate overseas. Whether any other countries will adopt the SHAKEN/STIR framework is unknown. What is known is that the unwanted calls will seek out the weakest link in the system. Because most robocalls originate in IP format, they can quickly be aggregated and rerouted as soon as roadblocks are instituted.

The SHAKEN/STIR framework also leaves open the issue of what carriers should, or are permitted to, do with the authentication information. Should unsigned calls be automatically blocked? Should it be left to the choice of the end user? How will that be implemented in conjunction with other tools that carriers and third parties are currently using to combat robocalls? As Sprint has previously noted, the most practical solution to unwanted robocalling on wireless networks is the use of applications that receive call analytic information from various sources—including complaint databases, routing information, and authentication information—and allow customers to choose whether unwanted calls should be blocked, sent to voicemail, or ring through to the wireless device.

Unfortunately, the immediate effect of SHAKEN/STIR is likely to be minimal. Small carriers are likely to lag large carriers in implementation. Any TDM link in the call flow will eliminate the ability to authenticate the call, and the nation is still many years away from all IP calling. And, as stated above, international traffic remains a great unknown. Until use of SHAKEN/STIR is ubiquitous, the fact that a call is signed or unsigned will have little predictive weight regarding the legality of a robocall. Most call recipients are unlikely to block all unsigned calls because it will be many years before the unsigned status of a call reflects that it likely to be an unwanted robocall.

II. User Choice Should Be Paramount in Battling Robocalls

When taking action in this area, the Commission must carefully weigh the costs and benefits of any regulatory requirements. Taking advantage of the capabilities of modern wireless devices is a more effective means of battling robocalls, both from a performance perspective and cost perspective, than mandating network based solutions. Fortunately, the Commission agrees and the proposed rules make such blocking voluntary and the use of SHAKEN/STIR voluntary while simultaneously paving the way for each carrier, device maker, mobile OS developer, app developer, or customer to manage their call flow in a way that makes sense to them.

Sprint is hopeful that call authentication will help carriers battle unwanted robocalls, but it is unlikely to be sufficient on its own to achieve the result desired by the Commission, carriers, and customers. Sprint is actively engaged in other ways to defeat unwanted robocallers. Sprint has partnered with Cequint to enhance its Premium Caller ID product that allows Sprint customers to subscribe to an optional, paid service that empowers Sprint customers to receive information about the type of caller that is attempting to reach them and to set up preferences to send those calls to voicemail or to block them entirely, category by category.

Sprint also recognizes that third-parties have created effective robocall prevention apps and encourages the Commission to enact policies that allow for this marketplace to develop rather than imposing a one-size-fits-all requirement that would have the effect of stifling such innovation. Device manufacturers and OS developers should be encouraged to facilitate the development of software—by carriers as well as app developers—so that customers can choose their preferred solution.

III. STIR/SHAKEN Is Only A Partial Solution

The Robocalling Strike Force noted that SHAKEN/STIR is but one of many mitigation

techniques that may be used to counter fraudulent calling. SHAKEN/STIR by itself does not actually prevent fraudulent calling; its output could be used to display some notification to the called party, but as noted in the NOI, there is as yet no standard for the interpretation of the output of SHAKEN/STIR to the called customer, and indeed it may not be possible to describe such interpretation in a technical standard that is meaningful to the consumer, other than a simple trust/doubt indicator. Otherwise the results from SHAKEN/STIR may be used for analysis, for example of calling patterns, but there are other sources of verified data that may be used for this, as noted by the Robocalling Strike Force.

SHAKEN/STIR does not provide assured indication of all malfeasant activities, rather only those that the bad actors may attempt using SHAKEN/STIR compliant carriers to both terminate and originate the calls. The effect of this will therefore be to drive bad actors to use unreliable and overseas carriers for their fraudulent originations. In the medium term, the effect of SHAKEN/STIR implementation will be to drive the bad actors from the compliant carriers, who generally have not been hosting them in the first place.

Finally, it must be realized that the industry does not yet know the impact of the implementation of SHAKEN/STIR on the cost of providing service. Of particular concern are the costs associated with the use of digital certificates. If, as is expected, SHAKEN/STIR implementation may require use of one certificate per telephone number, then the cost of certificate management may become prohibitive, or at least become very poor value in relation to the level of assurance provided.

IV. Framework for Evaluating the Effectiveness of Robocalling Mitigation Proposals

The eventual aim of any work to mitigate robocalling and the used of spoofed caller IDs to perform miscreant acts must be to reduce the incentive to do this to such a point that the issue

becomes insignificant, both as to its burden on carriers as well as the nuisance to individual customers.

To this end, a number of tools have been considered and created that can assist with such mitigation. In order to determine how each of these tools can be best applied, the full characteristics of each need to be considered:

- What reduction in spoofing will this tool allow?
- How easy is it for the robocallers to continue to place unwanted calls while avoiding the traps placed by any particular tool?
- What is the cost to the consumer and legitimate network operators to deploy the tool?
- What are the other downsides of deployment of the tool, such as prevention of delivery of legitimate calls that are wanted by the recipient?

Sprint is concerned that many of the tools that have been generated have not been well tested against these criteria, or at least their proponents have not always been willing to proffer their role in the overall strategy required to minimize spoofed robocalling.

Overall, a more fruitful approach to the robocalling problem is to determine how much mitigation is required to reduce the spoofed robocalling problem to insignificant levels and to examine how all available tools can be assembled to enable such mitigation, rather than examining the merits of each individually and trying to determine how the Commission's rules should be adjusted to enable or even require the use of each on its own. The ability of the bad actors to avoid the impacts of each tool, whether it's blocking or authentication, both alone and in concert with others, must be weighed against the cost to the industry and ultimately to the consumer of their implementation.

V. Conclusion

Sprint fully supports the Commissions actions to address the plague of unwanted robocalls. Neither carriers nor consumers benefit from the surge in unwanted calls and Sprint will continue to work with the Commission and the industry to find solutions to this complex problem. Sprint appreciates the Commission's actions here to empower carriers to protect their customers from unwanted robocalls.

Respectfully submitted,

SPRINT CORPORATION

_____

Charles W. McKee
Vice President, Government Affairs
Federal and State Regulatory

Keith C. Buell
Senior Counsel, Government Affairs
Federal Regulatory

900 Seventh St. NW
Suite 700
Washington, DC 20001
(703) 592-2560

September 13, 2017