BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

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

Comment of Professional Association for Customer Engagement

Filed July 24, 2019

Stuart Discount
Professional Association for
Customer Engagement
8445 Keystone Crossing, Suite 106
Indianapolis, Indiana 46240

Chief Executive Officer of Professional Association for Customer Engagement

Michele A. Shuster, Esq.
Nicholas R. Whisler, Esq.
Joshua O. Stevens, Esq.
Michael C. Dunn, Esq.
Mac Murray & Shuster LLP
6525 West Campus Oval, Suite 210
New Albany, Ohio 43054

Counsel for Professional Association for Customer Engagement

I. Introduction

The Professional Association for Customer Engagement ("PACE")[1] submits these comments in regard to the Commission's Third Further Notice of Proposed Rulemaking ("TFNPRM").[2] PACE continues to support the Commission's efforts to address the problem of robocalls, focusing the remedy on preventing illegal automated calls; however, PACE believes that any solution must be balanced against the harm of potentially blocking legal calls. The TFNPRM's proposed safe harbor should incentivize carriers to only block calls as authorized by the called party using SHAKEN/STIR-based blocking systems and take every reasonable step to prevent erroneous blocking. A critical call list would serve as a tool for spoofing creating an even greater public safety risk without being tied to call authentication. Lastly, although call authentication systems should be deployed as soon as possible, rapid deployment should not come at the expense of proper testing and calibration to prevent blocking of legal calls.

II. The Safe Harbor Should Incentivize Best Practices

PACE encourages the Commission to modify the safe harbor language of the Commission's proposed rule (i) to limit its scope to carriers that apply blocking standards in accordance with the called party's instructions, but due to unverifiable or missing SHAKEN/STIR[3] attestation data block a call that should not have been blocked had the SHAKEN/STIR attestation data been present and verifiable, (ii) to require that carriers provide mechanisms to inform callers and called parties when their calls are blocked and remove blocking that does not comport with the called party's instructions, and (iii) to be based on well-defined standards that comport with the limits of SHAKEN/STIR technology.

a. "Garbage In, Garbage Out"

PACE believes that a safe harbor should be limited to terminating carriers who correctly apply a SHAKEN/STIR-based blocking system, but erroneously block an otherwise permissible

[1] PACE is the only non-profit organization dedicated exclusively to the advancement of companies that us a multi-channel contract center approach to engage their customers, both business-to-business and business-to-consumer. These channels include telephone, email, chat, social media, web and text. Our membership is made up of Fortune 500 companies, contact centers, BPOs, economic development organizations and technology suppliers that enable companies to contact or enhance contact with their customers.

[2] Third Further Notice of Proposed Rulemaking, *In the Matters of Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Fed. Reg. Vol. 84, No. 121, 29478 (adopted June 6, 2019, published June 24, 2019).

[3] Signature-based Handling of Asserted information using toKENs ("SHAKEN"); Secure Telephony Identity Revisited ("STIR").

(*i.e.*, a call not of the type the called party has instructed the carrier to block) call due to erroneous or missing SHAKEN/STIR attestation information. First, because the terminating carrier is the carrier best positioned to know the called party's blocking instructions, it should be the only carrier permitted to block calls based on the called party's instructions.[4]

Second, blocking must only be based upon the called party's instructions to the carrier. For example, if the called party has instructed the carrier to only block calls with no attestation, an unverified attestation, or a gateway attestation, then the carrier must comply with those instructions. If the carrier in this example were to block a call with a verified partial attestation, then it would not be entitled to the safe harbor because it acted contrary to the called party's instructions.[5]

Third, but for the erroneous SHAKEN/STIR attestation (*e.g.,* the call should have received a full attestation but was only signed by the originating carrier with a gateway attestation; the call was signed using an expired certificate that caused verification to fail), or lack of SHAKEN/STIR attestation information, the call would have not been blocked by the carrier. Especially at the beginning of SHAKEN/SITR deployment, calls may lack SHAKEN/STIR attestation because of legacy telephone equipment failing to sign a call or causing a SIP-based INVITE call to have its Identity header stripped off during transit.

The Commission should limit the safe harbor's application as described above because of the substantial risk to called parties if their calls are erroneously blocked. Called parties could miss important calls, such as fraud alerts from their credit unions. They could miss calls from their doctors or pharmacists reminding them that their prescriptions are ready. People could fail to get notices that their packages had been delivered and find those packages stolen. It is important to keep in mind that people have medications, medical equipment, and other life-critical supplies delivered to their homes. In other words, erroneously blocked calls could become a real problem with lasting and devastating effects.

---

[4] *See, also*, Comment of Professional Association for Customer Engagement, *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59 (filed July 20, 2018) at 6.

[5] As more fully detailed in PACE's letters to Marlene H. Dortch on May 29, 2019 and May 30, 2019, PACE continues to object to call-blocking by default because of the lack of consumer choice and risk of improperly-blocked calls that an opt-out regime creates. Letters of Professional Association for Customer Engagement to Marlene H. Dortch, Secretary, Federal Communications Commission, *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59 (filed May 29, 2019 and May 30, 2019) (incorporated herein by reference).

b. Notification & Correction[6]

Under current call blocking regimes, the caller does not receive any notification that their call has been blocked. Likewise, no consistent standard exists for informing called parties that they did not receive a blocked call. This glaring gap in call blocking architecture presents real risks to both callers and called parties. For example, a doctor's office attempting to reach a patient with an urgent test result may constantly receive busy signals when their call is being blocked leaving them wondering how to reach the patient, and meanwhile, the patient may not receive any indication the doctor's office is trying to reach her. A safe harbor should not be provided to carriers who fail to put in place systems to remedy these issues.

First, the industry, working with the Commission, should designate a SIP error code and intercept message that would be used specifically to alert a caller that their call has been blocked by a carrier. Such error codes and messages have been used for decades and would be a relatively simple mechanism to provide notice to the caller using existing technology. If designating a new error code would prove unworkable, the Commission could designate that an existing unused or rarely used error code be re-designated for this purpose. The intercept message should also identify the carrier that blocked the call and contact information to obtain further information to remediate the potential error. Only carriers utilizing the approved caller notification method should qualify for the safe harbor.

Second, the called party needs a way to check if they are not receiving calls they desire. PACE believes real-time notification,[7] such as an online portal or smartphone application, is the best solution because it would allow the called party to check their blocked calls at any time. Alternatively, the carrier could provide a listing daily or weekly in an online portal. For consumers without online access, the carrier could offer a telephone-based portal, such as an IVR system, where a called party could access the same information. The Commission should set a minimum notification standard comprising at least one or a combination of the above recommendations.

After learning that a call has been erroneously blocked, the called party and the caller should be able to easily contact the carrier and resolve the error to prevent future blocking. PACE

---

[6] Additional discussion of notification and correction mechanisms can be found in Comment of Professional Association for Customer Engagement, *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59 (filed July 20, 2018) (incorporated herein by reference).

[7] Any notification should include at least the caller ID presented and the date and time of the call.

believes that the above-described safe harbor should only be available to the carriers that can show that they have a process in place for easily and quickly remediating erroneously blocked calls. At a minimum, each carrier should be required to publish on its website a toll-free number and email address that will connect a caller or called party with the carrier's error resolution team. The error resolution team should be available all day, every day. The carrier should be required to resolve the alleged error within twenty-four (24) hours of the report. For its part, the Commission could (i) implement a program to receive and work with carriers to resolve complaints of untimely or denied call-blocking error resolutions and (ii) require that carriers quarterly report aggregate statistics on call blocking remediation requests received and the outcome of those requests.[8] Without such a requirement, there would be nothing stopping a carrier from receiving the benefit of the safe harbor without expelling any effort to improve the SHAKEN/STIR framework by improving the security and accuracy of call attestation, which benefits carriers and consumers alike.

c. Well-Defined Standards

The TFNPRM conflates SHAKEN/STIR-based blocking with analytics-based blocking. The Commission should be careful to keep these concepts distinct. In a SHAKEN/STIR-based blocking system, all call blocking is based solely on SHAKEN/STIR attestation information. In an analytics-based blocking system, an analytics provider may or may not combine SHAKEN/STIR attestation information with other data points to determine the likelihood that a call is wanted/unwanted, or legal/illegal, and recommend or not recommend the carrier block the call. The Commission should only use terminology that reflects the content of the call (*e.g.*, wanted, unwanted, legal, illegal, presumably illegal), in reference to an analytics-based blocking system because SHAKEN/STIR alone does not provide any data reflecting on the content of the communication.[9] Further, to the extent a consumer opts-in or does not opt-out to a carrier's analytics-based program that attempts to categorize calls based on such subjective terminology, (i) carriers should not receive any safe harbor for erroneous blocking (because the safe harbor should

[8] A quarterly reporting mechanism would allow the Commission to identify carriers with unusually high numbers of requests which would indicate likely problematic blocking practices.

[9] For a detailed discussion of the different terminology applied in the SHAKEN/STIR-based blocking environment as compared to the analytics-based blocking environment, and the importance of using the correct terminology, *see*, Comments of Noble Systems Corporation, *In the Matters of Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97 (filed July 24, 2019).

be limited to SHAKEN/STIR-based blocking which is more objective) and (ii) callers should be permitted to challenge the subjective characterization of their call using the carrier's notification & correction procedures outlined above.

One example of the problem with conflating the two concepts can be found in the Commission's proposed safe harbor. The safe harbor proposed by the Commission would take into consideration a "failed caller ID authentication." Specifically, "[a] call would fail authentication when the attestation header has been maliciously altered or inserted."[10] Contrary to this statement, the SHAKEN/STIR framework is not designed to relay the intent of the party ("maliciously"), nor will it identify if an attestation header has "altered or inserted." Rather, SHAKEN/STIR will indicate whether the SIP Identity header contents can be verified and whether the caller ID is attested to, and if so, the level of attestation (full, partial, or gateway). Whether the attestation is legitimate will be determined by the terminating carrier using its encryption key to verify the cryptographic signature. PACE urges the Commission to be very careful in its creation of the safe harbor and in its related discussions of call blocking technology to maintain an appropriate distinction between SHAKEN/STIR-based blocking and analytics-based blocking.

III. Critical Call List Drawbacks & Solutions

The Commission should carefully consider the ramifications of a Critical Call List.[11] A Critical Call List would create a list of exempted numbers ripe for spoofing since they would be white-listed from blocking. Imagine a scam artist spoofing the number of the local police department or fire department and being incentivized to do so because the scammer knows the call will be allowed to connect. The public would not be able to trust calls from emergency services and could easily be taken advantage of by the scammers.

[10] TFNPRM at ¶ 3.

[11] The Commission also seeks comments on the types of numbers that should be included on a Critical Call List. PACE recommends that callers representing entities forming the backbone of emergency services should be included (*e.g.*, police departments, fire departments, health departments, hospitals, departments of emergency management, and similar agencies). The Commission should also consider including entities that represent core services to the public and which disruptions or incidents related to such services would pose a health or safety risk (*e.g.*, utilities, telecommunications providers, schools, and departments of transportation). To prevent misuse of the privileges associated with being included on a Critical Call List, the Commission should require listees to utilize listed numbers only for calls related to matters that could affect the health & safety of the called party or public at-large (*e.g.*, severe weather alerts, natural or man-made disasters, active shooter incidents, lock-downs, and utility outages).

In order to prevent this nightmare scenario, a carrier that utilizes an analytics-based blocking system[12] could use SHAKEN/STIR authentication in conjunction with a Critical Call List and require that the call both purport to be from a Critical Call List number and be accompanied by a full attestation to exempt it from other analytics-based blocking criteria.[13] Unfortunately, as the Commission indicated in the TFNPRM, not all carriers will have deployed SHAKEN/STIR by the end of 2019. More than likely, although major carriers will have completed deployment, smaller carriers primarily serving rural and underserved populations will not. Emergency services utilizing smaller carriers would be at risk from this proposed solution because their calls would be blocked.

The Commission should consider a middle ground approach that holistically identifies and permits critical calls. A Critical Call List should be created and maintained by the Commission. Carriers should be required to take a number's including on the List into account when applying analytics algorithms; however, List inclusion should not serve as the only factor. Carriers should also take into account the SHAKEN/STIR attestation rating associated with the call (if any) and factors such as calling patterns, originating carrier, reports of emergency situations in the area where the called party is located, and other factors associated with the likelihood that the caller is or is not who they purport to be. After SHAKEN/STIR has been fully implemented across all carriers, then the combination of listing on the Critical Call List and a full SHAKEN/STIR authentication could serve as the litmus test for blanket permission to connect. By allowing carriers to dynamically respond to multiple variables, the Commission would reduce the risk of scammers spoofing numbers listed on the Critical Call List whilst simultaneously preserving the ability of critical callers not served by carriers who have adopted SHAKEN/STIR to make critical calls to their community.

IV. Caller ID Authentication Should be Mandated Over Time

PACE wholeheartedly believes that SHAKEN/STIR and future similar caller ID authentication solutions should be deployed across all telecommunications networks, but

[12] Theoretically, any call with full attestation under SHAKEN/STIR would not be blocked in a SHAKEN/STIR-based blocking system.

[13] The Commission asks whether keeping the Critical Call List non-public would avoid unlawful spoofing. TFNPRM at ¶ 14. Because a scammer could reasonably determine numbers that would be on the List because they would know the bases for inclusion on the List, hiding the List from the public would not have a material effect on the risk of illegal spoofing of numbers on the list and is outweighed by the public's right to know numbers included on the List.

recommends the Commission allow sufficient time for testing and correction prior to and during deployment. Without broad deployment, SHAKEN/STIR attestation ratings cannot serve as a valuable data element in analytics algorithms, or, if pressured by the public or the Commission to place too much weight on SHAKEN/STIR attestation ratings too quickly, millions of legal calls could be summarily blocked.[14] Even as it stands today, according to an analysis by Global Wireless Solutions, Inc. and Hiya (a provider of call-blocking solutions), the algorithms in use by the three main analytics companies have error rates of 0.25%-1.48%.[15] Put in context of a telecommunications system with tens of billions of calls per year, that means many millions of calls could be erroneously blocked (*e.g.*, a wanted call designated as unwanted and blocked) under analytics-based call blocking systems used by many of the carriers at this time. The Commission simply should not rush deployment of technology that is still in its infancy with the potential to cause such harm.

America's largest carriers, specifically, AT&T, Verizon, Comcast, T-Mobile, Sprint, Charter, Cox, and Vonage, have already noted that they expect to implement SHAKEN/STIR on aggressive timeframes, and some by the end of 2019. PACE believes these carriers constitute the "major voice service providers" the Commission seeks to identify. If the major voice service providers have not in fact met their goal of implementation[16] by 2019, PACE believes it would be appropriate to mandate they complete deployment by the end of 2021 because these carriers have the resources available to work out the bugs in the system and finish implementation (they have also been involved in the development of the technology from the start so they have had the longest period of time to understand and implement it).

On the other hand, smaller carriers primarily serving rural and underserved populations do not have the resources of the major carriers. The Commission should allow additional time to these smaller carriers. PACE would recommend giving them an additional two to three years after full implementation by the major carriers.

---

[14] As noted in the section above, carriers using SHAKEN/STIR-based blocking would not be affected by mis-weighting since they do not apply analytics algorithms to determine whether to block a call.

[15] *First-of-its-Kind Study Ranks Spam Detection Providers' Ability to Accurately Detect Unwanted Robocalls*, BusinessWire (May 9, 2019), available at: https://www.businesswire.com/news/home/20190509005215/en/First-of-its-Kind-Study-Ranks-Spam-Detection-Providers'-Ability (last accessed July 15, 2019).

[16] PACE believes that "implementation" should mean that the carrier is capable of (1) cryptographically signing calls originating on its network, (2) receiving and correctly interpreting signatures from other carriers, and (3) incorporating signature information into its call-blocking and labeling algorithms.

V. Conclusion

The Commission should use the proposed safe harbor to incentivize carriers to only block as authorized by the called party using SHAKEN/STIR-based blocking systems and take every reasonable step to prevent erroneous blocking. This means limiting the safe harbor to carriers that (i) act appropriately, but due to unverifiable or missing SHAKEN/STIR attestation data block a call that otherwise would have connected to the called party and (ii) provide mechanisms to inform callers and called parties when their calls are blocked and rectify erroneous blocking. The Commission could also adopt a Critical Call List for carriers using analytics-based call blocking systems to utilize as a data point in their call-blocking algorithms, but inclusion on the List should not serve as a standalone basis for exemption from call blocking. Finally, although call authentication systems should be deployed as soon as possible, rapid deployment should not come at the expense of proper testing and calibration.

Respectfully submitted,

Michele A. Shuster, Esq.
Nicholas R. Whisler, Esq.
Joshua O. Stevens, Esq.
Michael C. Dunn, Esq.
Mac Murray & Shuster LLP
6525 West Campus Oval, Suite 210
New Albany, Ohio 43054
Telephone: (614) 939-9955
Facsimile: (614) 939-9954