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

REPLY COMMENTS OF SPOOFCARD LLC

Mark C. Del Bianco
Law Office of Mark C. Del Bianco
3929 Washington St.
Kensington, MD 20895
301-602-5892
mark@markdelbianco.com

Amanda Pietrocola
CEO
SpoofCard LLC
101 Crawfords Corner Road
Suite 1230
Holmdel, NJ 07733

August 22, 2019

Table of Contents

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

Introduction

SpoofCard LLC ("SpoofCard") submits these reply comments in response to the Third Further Notice of Proposed Rulemaking ("*Third FNPRM*") in the above captioned dockets and in reply to the comments filed in response thereto. [1]

SpoofCard owns and operates SpoofCard.com, a PSTN voice service that operates like a regular long distance calling card service, but with additional capabilities, including providing each customer the capability to alter the Caller ID that is displayed on a called party's telephone. See <www.SpoofCard.com>.

SpoofCard has a unique perspective in this debate. The SpoofCard service is used by individuals, law enforcement agencies and small and medium-sized businesses ("SMBs") to obtain the type of caller ID masking or spoofing capability that large businesses obtain through the use of PBXs and cloud-based universal communications services. For reasons explained in more detail below, SpoofCard.com is not (and could not economically be) used to make robocalls.

[1] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*; *Call Authentication Trust Anchor*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51 (2019). Paragraphs 22-44 of the *Third FNPRM* are referred to as the "*Declaratory Ruling*".

The SpoofCard service was developed by TelTech Systems, Inc. in 2007. SpoofCard LLC was spun off from TelTech and sold to new owners in 2018. Since the inception of SpoofCard.com over a decade ago, SpoofCard and TelTech have devoted substantial resources to keeping bad actors—including parties engaged in fraudulent or harmful spoofing—from abusing their platform.

Over the last 12 years, SpoofCard and TelTech have developed and adopted a number of safeguards that largely prevent SpoofCard.com customers from making unlawful spoofed calls from the platform. These safeguards have included:

- a strong prohibition in the terms of service on placing unlawful or unwanted calls through the platform;
- billing by the minute, rather than by the second, in order to deter short-duration calls and impair the economics of unlawful robocalls;
- always requiring manual dialing of calls placed on the service and never enabling automated dialing;
- development and implementation of some of the earliest "do not spoof" lists that prevent spoofing of the numbers of the Internal Revenue Service, law enforcement agencies and other entities;
- development and implementation of some of the earliest "do not call" lists that prevented spoofed calls from going to 911 centers, money transfer companies, banks and other key institutions; and
- pioneering the early use of artificial intelligence and data analytics to identify risk vectors, monitor patterns that might indicate abuse, and respond to complaints.

These safeguards allow SpoofCard to detect bad actors that attempt to misuse its platform and equip it with the legal tools necessary to take swift action against those actors.

TelTech and SpoofCard also have a long history of working with Congress and the Commission to craft caller ID spoofing laws and regulations that balance the competing interests of legal spoofing users and the need to prevent robocalls, and of working with federal and state law enforcement to address illegal uses of caller ID spoofing. In 2009 and 2010, for example, TelTech worked with staff of both the House and Senate to develop what became the Truth in Caller ID Act of 2010. TelTech subsequently participated in the Commission rulemaking that resulted in the regulations implementing the Act. Those regulations tracked closely the recommendations made by TelTech in its comments.

TelTech and SpoofCard also have a long record of proactive co-operation with law enforcement. SpoofCard.com is widely used by law enforcement customers because of its call-by-call flexibility, and some of its largest customers are law enforcement agencies and personnel. In addition to responding annually to dozens of subpoenas and search warrants from U.S. law enforcement, TelTech and SpoofCard have co-operated through international legal channels with law enforcement agencies from numerous other countries. In addition, SpoofCard and TelTech have provided training sessions for U.S. law enforcement and prosecutorial personnel on the mechanics of caller ID spoofing and on fraudulent and other illegal uses of caller ID spoofing.

SpoofCard strongly supports the Commission's efforts to protect consumers against robocalls. It believes that the *Declaratory Ruling* and the *Third FNPRM* are positive steps towards solving the robocall problem. However, as all commenters acknowledge, robocalls are a complex, dynamic and ever evolving challenge. There is no magic bullet that provides a lasting solution.

Summary

SpoofCard, like rural carriers, enterprise customers and other marginalized groups in the voice services ecosystem, runs the very real risk that hasty and piecemeal Commission action to try to stem the flow of robocalls could cause many of its customers' legal calls to be blocked.

There is presently no basis to allow voice providers to block calls simply because the calls may fail Caller ID authentication under SHAKEN/STIR. The SHAKEN/STIR framework certainly cannot now be used - and probably should never be used - as the sole basis for a network-wide opt out blocking regime. Given the practical shortcomings of the SHAKEN/STIR framework, the Commission also should not implement a safe harbor for blocking based just on a SHAKEN/STIR authentication failure. Because so many legal calls would inevitably be blocked, absent substantial future changes to the SHAKEN/STIR framework, such such blocking and any associated safe harbor would violate the Communications Act's mandate that the Commission ensure that legal calls are completed.

Instead, the Commission should focus on and encourage the further development of analytics-based frameworks for call blocking. If it is not willing to consider a safe harbor for analytics-based blocking now, it should monitor the technological developments in this area and when it believes the levels of accuracy warrant, should create such a safe harbor.

I. The Commission Should Not Allow Call Blocking Based Solely On A Failure of Authentication under SHAKEN/STIR

The Commission has proposed to give teeth to the SHAKEN/STIR framework by greenlighting voice service providers to offer "call-blocking programs that take into account whether a call has been properly authenticated under the SHAKEN/STIR framework and may potentially be spoofed."[2] While the Commission's goal is laudable, blocking calls based on failed authentication is not a reasonable means to achieve the goal.

The SHAKEN/STIR framework operates by having originating voice service providers electronically sign a certificate attesting to the authentication of the calling number. The framework contemplates three levels of attestation based on the originating provider's level of confidence that the calling party is authorized to use the number that would be presented in the

[2] *See Third FNPRM at* ¶¶ 46-51. There is some ambiguity in this section of the *Third FNPRM*, which originally refers to call blocking programs that generally "***take into account*** whether a call has been properly authenticated under the SHAKEN/STIR framework." ¶ 46 (emphasis added). If the Commission is considering a safe harbor for multi-factor call blocking analytics programs in which failure of SHAKEN/STIR authentication is but one input, SpoofCard would support such an approach, as discussed in Part III below.

Caller ID field.[3] The Commission proposes to define a failure of authentication under SHAKEN/STIR as a failure of a call to have any of the three levels of attestation.

The intractable problem with the Commission's proposal, as many commenters have pointed out, is that calls that are perfectly legal and are not robocalls can "fail" SHAKEN/STIR protocol authentication. This is to be expected, since SHAKEN/STIR authentication was never intended to serve as a proxy for the legality or illegality of calls.[4] Rather, it was and still is envisioned by the technical groups developing it as "one of the tools that can reduce illegal robocalls."[5] Even USTelecom, the trade group for the large carriers (some of whom are pushing hard for the immediate right to implement network-wide blocking based solely on a failure of authentication under SHAKEN/STIR[6]), admits that standard is not designed – and was never intended – to determine a caller's intent or on a stand-alone basis or to be used to automatically keep calls from completing.[7]

Authentication results under SHAKEN/STIR are presently unreliable in identifying illegal calls and will remain so for the foreseeable future.[8] There is serious question among voice service providers and other stakeholders about whether, even with suitable modifications

[3] Those levels of attestation are full, partial and gateway. *See* Joint ATIS/SIP Forum Standard – Signature-Based Handling of Asserted Information Using toKENs at 8, https://www.atis.org/stiga/resources/docs/ATIS-1000074.pdf .

[4] The framework's purpose was to assist with traceback efforts to identify an originating carrier and it does not determine whether a call is legal or illegal or wanted or unwanted.

[5] Comments of NTCA - the Rural Broadband Association, at 12, 13-14 ("NTCA Comments"); Comments of the Voice on the Net Coalition, at 1 ("VON Comments"); Comments of USTelecom, at 2 and 6-7 ("USTelecom Comments"); and Comments of Transaction Network Services, Inc. at 4-6 ("TNS Comments"). Unless otherwise noted, all references to "Comments" are to comments filed by a party on July 24, 2019 in response to the *Third FNPRM*.

[6] *See, e.g.,* Comments of AT&T Corp. at 19-23 ("AT&T Comments").

[7] USTelecom Comments at 6-8.

[8] NTCA Comments at 12, 13-14; see also VON Comments at 1; USTelecom Comments at 2 and 6-7; TNS Comments at 4-6; and Comments of First Orion Corp. at 3-4 ("Authentication results will be unreliable in the near term. Authentication results will be more reliable in the long term, but still will not serve as a good proxy for the legality or illegality of calls.")

in SHAKEN/STIR's development and implementation, the framework will *ever* be able to sufficiently accurately identify illegal calls so as to justify its use as a blocking proxy.

Blocking based solely on failure of SHAKEN/STIR authentication would be both underinclusive and overinclusive in identifying illegal calls. The underinclusive aspect can readily be remedied by adding additional analytics- based factors to a call blocking algorithm. The overinclusiveness - the blocking of many legal calls that are not robocalls simply because they lack authentication - is a much more important and potentially costly problem, both monetarily and in terms of non-monetary societal harm.

Particularly during the initial years of SHAKEN/STIR implementation, when there is not universal adoption by all participants in the voice ecosystem and numerous TDM networks remain in operation, there will be a high percentage of calls where there is no attestation or certificate at all.[9] The reasons for the lack of authentication can vary, but many are going to be related to a lack of end-to-end IP connectivity. For example, if a service provider in the call chain uses TDM technology, there is no possibility for the end-to-end transmission of any certificate issued by the originating provider and such a call will never be authenticated under SHAKEN/STIR.[10] In addition, SHAKEN/STIR does not presently incorporate other types of non-carrier entities, including over the top (OTT) voice services providers and enhanced service providers who serve enterprise customers.[11] Another group whose calls will not be authenticated will be enterprises, who are unable to sign their own certificates under SHAKEN/STIR as it is

[9] *See, e.g.,* Comments of the American Association of Healthcare Administrative Management, at 4-5 ("AAHAM Comments"); First Orion Comments at 4-6; Comments of INCOMPASS at 7-10 ("INCOMPASS Comments"); Comments of Competitive Carriers Ass'n, at 4-6 ("CC Ass'n Comments").

[10] *See, e.g.,* INCOMPASS Comments at 8.

[11] *See, e.g.,* Comments of Cloud Communications Alliance at 5-7 ("CCA Comments") and Comments of Telnyx LLC at 1-2 ("Telnyx Comments").

presently designed.[12] These enterprises' situation is exacerbated if they use multiple networks to originate calls. There are numerous other participants in the voice services ecosystem that cannot self-authenticate their calls under SHAKEN/STIR as it presently exists.

If blocking based on failure to authenticate is implemented, a not-insubstantial percentage of the unauthenticated calls will be legal calls. Therefore, while the Commission may be correct in expecting "the vast majority of calls blocked in such circumstances to be illegitimate," even a small percentage of false positives would result in hundreds of thousands or millions of blocked legal calls.[13] The costs of such false positives are great, but are inexplicably given short shrift by the Commission in the *Third FNPRM*.[14]

Everyone is aware of the dangers involved in inadvertent blocking of 911 callbacks and other emergency calls. Twilio in its comments summarizes the numerous additional vital use cases that could be improperly impeded if such blocking is implemented:

> Many of Twilio's legitimate services are at risk of being erroneously blocked or mislabeled by overbroad call-blocking criteria or algorithms. For example, Twilio's APIs are used to facilitate anonymous communications, which is an important safety feature in many scenarios. Ride-share passengers on Lyft and Uber, hosts and guests on Airbnb, users of the dating website eHarmony, and victims of domestic abuse all rely on Twilio's products to communicate safely without having to disclose their phone numbers to strangers. Twilio's platform also is used for crisis communications—supporting mass notification systems so that schools, businesses, governments, and other organizations can quickly and effectively communicate in a moment of crisis. Twilio also helps legitimate businesses and banks to deliver important notifications to their customers.[15]

[12] CCA Comments at 5 and Telnyx Comments at 2.

[13] There are already millions of incorrectly blocked legal calls. *See, e.g.,* Comments of Twilio LLC at 6 ("Twilio Comments"); Comments of Professional Association for Customer Engagement at 8; Comments of Credit Union National Ass'n, at 5-6 ("CUNA Comments") ("The record in this proceeding provides ample evidence that legitimate calls currently are being blocked and/or mislabeled and the incidence of false positives is likely to grow as blocking expands.").

[14] *Third FNPRM* at ¶ 48. *See* CUNA Comments at 8-9.

[15] Comments of Twilio LLC at 5 and 7.

The calls made by SpoofCard's customers, like those in the Twilio use cases and those made by emergency service providers and hospitals, are often critical for the called party. The costs of false positives (i.e., legal calls that are blocked) transcend monetary issues. Many of the harms can literally be life or death matters.

The Commission need not attempt to measure now the costs and benefits of allowing SHAKEN/STIR blocking because it is obvious that the number of incorrectly blocked legal calls will be so great that such call blocking would violate the Communications Act's requirement that legal calls be completed.[16] At a later time, when there is near-universal implementation of SHAKEN/STIR, the Commission could reconsider whether to allow call blocking based largely on failure of SHAKEN/STIR authentication. But that time is years in the future.[17] Although some larger carriers have begun to implement SHAKEN/STIR, the framework's governance structure and certain essential standards are still under development.[18] The framework will not be implemented by enterprises or the smaller carriers for years, due to the need for further development of the protocols and to costs and other factors, particularly the fact that most small carriers are still operating TDM-based networks.[19]

The Commission also needs to consider that carrier-based blocking based solely on failure of SHAKEN/STIR authentication will expand the existing incentives and opportunity for anti-competitive conduct by the large voice service providers, who will be the first to implement SHAKEN/STIR. They will be able with impunity to block calls that use third party number substitution or spoofing services (such as SpoofCard) and favor their own competitive services. They will also have the ability to block calls made by enterprise users and by the customers of

[16] *See* 47 U.S.C. §§ 201(b) and 202(a); and CUNA Comments at 10-11 and Numeracle Comments at 5.

[17] *See, e.g.,* WTA Comments at 3-6 and Cloud Communications Alliance Comments at 8-9.

[18] *See, e.g.,* VON Comments at 2-3.

[19] *See, e.g.,* WTA Comments at 3-6 and NTCA Comments at 3-10.

smaller voice communications providers that have not adopted SHAKEN/STIR, in order to cause the enterprises and customers to move to the large voice communications providers' services.

For all these reasons, SpoofCard agrees with the commenters who have demonstrated why there never should be blocking based solely on failure of SHAKEN/STIR authentication.[20] However, the Commission need not address that issue in 2019. It is sufficient to recognize that such blocking cannot be implemented at this time.

II. The Commission Should Not Create a Safe Harbor for Blocking Unauthenticated Calls

Given all of SHAKEN/STIR's shortcomings, there is presently no basis for the Commission to find "call-blocking programs targeting . . . calls [that fail SHAKEN/STIR authentication] to be deserving of safe harbor."[21] Because the Commission cannot require or even permit network-wide call blocking based solely on a failure of SHAKEN/STIR authentication, there is no need at this time to consider whether the Commission should create a safe harbor for voice providers implementing such blocking.[22]

If the Commission were nonetheless to decide to implement such a safe harbor, the safe harbor would for years inevitably have to be very limited. The Commission recognizes that such a safe harbor should only apply for blocking calls where the authentication framework has been fully implemented and is available for use throughout the call chain.[23] Given this constraint, for a long period of time (at a minimum several years, as discussed above) any such safe harbor could not possibly apply to large swaths of PSTN voice traffic.[24]

[20] *See, e.g.,* Comments of West Telecom Services, LLC at i-ii and 13-16; WTA Comments at 3-6; and USTelecom Comments at 6-8.

[21] *See Third FNPRM* at ¶ 48 and First Orion Comments at 4.

[22] Comments of ACT | The App Association at 5-6.

[23] *See Third FNPRM* ¶ 50.

[24] *See*, *e.g.* VON Comments at 2-3.

Furthermore, any safe harbor implemented by the Commission should apply only to voice service providers that implement call blocking on a competitive- and technology-neutral basis. Adopting this common-sense condition will help speed up the implementation of SHAKEN/STIR and ensure that the adoption of any blocking regime - whether or not it is analytics-based - is a tool for empowering and protecting consumers, and not for entrenching the position of the largest voice service providers.[25]

III. The Commission Should Consider Allowing Network-wide Blocking Based on Reasonable Analytics

SpoofCard agrees with those commenters who contend that the Commission should only allow carrier-based opt out blocking based on reasonable analytics factors, such as those used by RoboKiller, Transaction Network Services and First Orion, among others.[26] Almost any analytics-based system will be more accurate than the simplistic SHAKEN/STIR authentication test. Most importantly, a system based on the factors or indicia of robocalling identified in the *Third FNPRM* will have significantly fewer false positives than the SHAKEN/STIR authentication test. In other words, there will not be the societal costs of millions of blocked legal calls.

The Commission should focus on and encourage the further development of analytics-based frameworks for call blocking. It should closely monitor the technological developments in this area and when it believes that the levels of accuracy warrant, should institute a safe harbor for analytics-based call blocking at the network level. Such blocking could be based on a variety of analytics, including but not limited to those identified in the *Third NFPRM*. But before a safe

[25] *Declaratory Ruling* ¶ *35;* West Telecom Comments at 13-16 and Twilio Comments at 10.

[26] *See, e.g.,* NTCA Comments at 12-13 and USTelecom Comments at 6-9.

harbor can be implemented for a particular analytics-based program, there must be rigorus analysis of the accuracy of the program's false positive rate. Otherwise, a broad safe harbor will encourage sloppy analytics and analysis, and create unacceptably high costs for society at large. In addition, before a safe harbor based on analytics can be permitted, there must be a critical calls list for non-blockable numbers, a requirement for real time notification of the blocking to the calling party and the service provider (e.g., SpoofCard), and a mechanism to ensure that calls from carriers and entities that are incorrectly blocked can quickly be unblocked.

Conclusion

SpoofCard strongly supports the Commission's efforts to combat unlawful robocalls and, in particular, to foster implementation of SHAKEN/STIR. But the blocking and safe harbor proposals in the *Third FNPRM* do not strike the right balance. They fail to consider the inherent shortcomings of the SHAKEN/STIR framework or the substantial costs and societal harm of the millions of wrongly blocked calls that will inevitably result from use of a single, narrow factor as a basis for network-wide blocking.

Respectfully submitted,

_________/s/_______________
Mark C. Del Bianco

Law Office of Mark C. Del Bianco
3929 Washington St.
Kensington, MD 20895
Tel: 301-602-5892
mark@markdelbianco.com

Amanda Pietrocola
CEO
SpoofCard LLC
101 Crawfords Corner Road
Suite 1230
Holmdel, NJ 07733