Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Caller ID Authentication Best Practices	)	WC Docket No. 20-324
	)	

COMMENTS OF YOUMAIL, INC.

YouMail, Inc. ("YouMail"),[1] through counsel, respectfully submits its comments in response to the Federal Communications Commission's ("Commission" or "FCC") Public Notice inviting comments on Caller ID authentication best practices.[2]

I. Introduction and Background

A. Best Practices

As the Commission states, the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act[3] requires the Commission, by December 30, 2020, to issue "best practices that providers of voice service may use as part of the implementation of effective call

[1] YouMail provides security-first, cloud-based communication services for mobile phones. Its free app-based service uses sophisticated, patented technology to block robocalls and phishing messages, protecting users from spam, identity theft, stalkers, and corporate fraud. YouMail's premium call management services provide virtual receptionist and virtual number services, and are designed for people who use their mobile phones for business. These services help customers unify virtual numbers with their cell number, handle high volumes of mobile calls, and provide personalized answering experiences for their callers. YouMail's communications platform handles over a billion calls per year for over 10 million users, and its users range from everyday consumers to sole proprietors to the CEOs of the largest companies in America. YouMail is privately funded and based in Irvine, California.

[2] Public Notice, "Wireline Competition Bureau Invites Comment on Caller ID Authentication Best Practices," WC Docket No. 20-324, DA 20-1154 (rel. October 1, 2020) ("*Notice*").

[3] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, S.151, 116th Cong., Pub. Law No. 116-105 (2019) ("TRACED Act").

authentication frameworks … to take steps to ensure the calling party is accurately identified."[4] The Wireline Competition Bureau charged "the Call Authentication Trust Anchor (CATA) Working Group of the NANC [North American Numbering Council] to recommend a set of best practices that would, in the NANC's view, satisfy Congress's direction if adopted by the Commission."[5] The Working Group's document was approved by the NANC on September 24, 2020 and is now before the public for comment. The *Notice* seeks comments on seven best practices proposed by the NANC and "any additional or alternative best practices commenters would recommend to achieve the TRACED Act's goal of ensuring the calling party is accurately identified."[6]

B. Extension of the STIR/SHAKEN Compliance Date for Small Service Providers

During this same time period, the Commission adopted new rules "to further promote implementation of the STIR/SHAKEN caller ID authentication framework to protect consumers against malicious caller ID spoofing."[7] "Among other things, [the FCC] adopt[ed] rules governing intermediate providers and caller ID authentication in non-IP networks, … implement[ed] the exceptions and extensions established by the TRACED Act, and … prohibit[ed] line-item charges for caller ID authentication."[8]

In recognition of the current marketplace reality that many small providers are, technically, practically, or otherwise unable to satisfy the requirements for full participation in STIR/SHAKEN, the Commission granted certain extensions from the June 30, 2021 compliance deadline:

> (1) a two-year extension to small, including small rural, voice service providers; (2) an extension to voice service providers that cannot obtain a certificate due to the Governance Authority's token access policy until such provider is able to obtain a certificate; (3) a one-year extension to services scheduled for section 214 discontinuance; and

[4] *Id.* at § 4(b)(7).

[5] Letter from Kris Anne Monteith, Chief, Wireline Competition Bureau, FCC, to Jennifer K. McKee, Chair, NANC (Feb. 27, 2020), https://docs.fcc.gov/public/attachments/DOC-362809A1.pdf.

[6] *Notice* at 1.

[7] *Call Authentication Trust Anchor*, Second Report & Order, WC Docket No. 17-97, FCC 20-136 (rel. October 1, 2020) ("*Trust 2nd R&O*").

[8] *Id.* at ¶ 4.

> (4) as required by the TRACED Act, an extension for the parts of a voice service provider's network that rely on technology that cannot initiate, maintain, and terminate SIP calls until a solution for such calls is reasonably available.[9]

However, the *Trust 2nd R&O* requires each service provider receiving such extension to "implement a robocall mitigation program to combat the origination of illegal robocalls during the course of the extension."[10]

II. Service Providers Must Take Effective Action Now

The scourge of illegal and unwanted robocalling and the fraud-related activities associated therewith are inflicting damage to the utility and value of voice communications in the United States. Many people receive vastly more illegitimate robocalls than legitimate, authorized, or otherwise lawful and desirable ones. Many people will not even answer their phones unless they are absolutely certain as to the identity of the caller. Congress, the Commission, industry groups and the public have consistently and repeatedly decried: "Fix this now!"

YouMail believes the "Best Practices" recommended by the NANC are a positive step forward. But best practices are only effective when they are: (1) achievable, (2) affordable, (3) adopted widely throughout the industry, and (4) readily and equitably enforceable. Absent some consensus and guidance from the government around the need for more immediate adoption of existing market-based technology solutions capable of mitigating illegal and unwanted robocalling, the main challenge with the current Best Practices proposal is that "years" (and not merely "months") will likely pass by before yielding meaningful improvements to a consumer's experience vis-à-vis robocall mitigation and reduction. Rolling out compliance plans over a period of years will permit fraudsters and other abusers of the telecommunications networks to continue preying on the public and degrading the utility and value of voice communications even further. Service providers should, therefore, be encouraged to use currently available technology solutions as part and parcel of the Best Practices adopted by the

[9] *Id.* at ¶ 38.

[10] *Id.*

Commission. Equally important is the need for near-real-time identification of "bad" calls and their sources, with the ability to shut down these sources in days, not weeks or months.

Many of the largest service providers, be they incumbent carriers, competitive carriers or interconnected VoIP providers, have implemented or are close to implementing STIR/SHAKEN. Many have also taken other steps to vet their upstream customers, both retail and wholesale (Best Practice No. 1), including international providers (Best Practice No. 6), and to implement supplemental robocall mitigation programs (Best Practice No. 7). They are not alone. A significant number of smaller carriers and VoIP providers, including those that use VoIP technology to provide commercial communications platforms, are implementing STIR/SHAKEN directly or are making arrangements for larger providers to sign the smaller operators' calls.

Given the need for at least some action sooner, rather than later (even by "small" providers), it is important that the Commission consider requiring or incentivizing such providers to do more than simply agree to implement certain practices at a future date. The conclusion in the *Trust 2nd R&O* that a number of service providers would experience "undue hardship" in meeting the June 30, 2021 deadline for full STIR/SHAKEN compliance is clearly not considered to be a 'blank check' by the Commission. Quite the contrary, as the Commission requires "any voice service provider that receives an extension to implement and certify that it has implemented a robocall mitigation program by June 30, 2021."[11] YouMail focuses the remainder of its comments and suggestions on the fleshing out of an effective robocall mitigation program.

III. Small Service Providers Must Implement Efficient, Effective and Readily Achievable Robocall Mitigation Programs

Today's technology permits small providers to take steps now to implement solutions that will mitigate robocalling. Critically, such technology enables providers small and large to do so efficiently, effectively and in a readily achievable manner. The STIR/SHAKEN framework is intended to help

[11] *Id.*

service providers know better their upstream customers (both retail and wholesale) as they receive, handle and pass along voice calls into the communications network. Logically, smaller carriers receiving an extension should implement mitigation programs (Best Practice No. 7) that also help service providers know their upstream customers (both retail and wholesale) better. These programs must include provider efforts to know the details of the traffic they originate or transmit and use such information to identify and curtail harmful traffic and their source. Smaller service providers need not "reinvent the wheel," as a number of vendors, including YouMail, offer wholesale services that enable this type of robocall mitigation.

YouMail's retail robocall identification and blocking service enables the Company to identify the characteristics of "bad calls" from its analysis of the billions of calls received by YouMail customers.

> When a call is made to our customer, our patented technology automatically compares the caller against our library of millions of bad behaviors and characteristics. If there's a match, we'll instantly send the call to a greeting that says "this number is not in service" greeting. The index works by extrapolating the data collected from the many tens of millions of calls made each month to YouMail users.[12]

YouMail protects 350 million phone numbers and has stopped more than a billion robocalls, while answering well over 10 billion calls to date.[13]

A robocall mitigation program reliant upon mid-to-high traffic volumes to identify bad actors would be effective for only those service providers that handle such high traffic volumes. It will not work for smaller providers, be they a rural telephone company or small, specialized business platform operator that incorporates VoIP calling. An alternative solution for these small providers is to use robocall mitigation programs that can identify and remove bad calls and their sources based on a lower number of calls.

[12] How does YouMail stop robocalls?, available online at https://www.youmail.com/home/feature/stop-robocalls (October 15, 2020).

[13] *Id.*

YouMail's system can be used by enterprise customers and service providers of all sizes. Because of YouMail's database of bad calls and their characteristics, coupled with YouMail patented technology, it no longer takes a service provider weeks or months to identify bad calls and their sources for further investigation. It also no longer takes sampling of thousands of calls from the same suspicious telephone number over a period of weeks. Rather, bad calls and their sources can be identified with a single call that shares identifiable characteristics with millions of other bad calls already analyzed and classified. It is "DNA" for voice traffic that identifies robo- and fraudulent calls based on one call matching the characteristics of other previously identified bad traffic. Instead of investigating thousands of sample calls over weeks, the service provider can complete its investigation, work with other service providers, regulatory and law enforcement agencies and have the source shut down in days.

Moreover, while robocallers and other fraudsters will soon alter their malevolent plans and begin another round of calling, quicker shutdowns of these schemes can greatly reduce the length of time a new scheme can continue. This, in turn, reduces ill-gotten financial gains and the incentives to engage in robocalling and wire fraud. Quick identification and shutdown of this traffic significantly reduces the benefit/cost ratio for illegal and unwanted robocallers. With quick identification and shutdown of bad actors, a two-month campaign of fraud and harassment can be limited to a one-week campaign.

IV. Measurement and Reporting Must be a Part of Any Robocall Mitigation Plan

Consumers and regulators alike must be able to know which service providers are successfully suppressing robocalls and which are not. Measurement also provides information as to which mitigation techniques work and which do not. Accordingly, the Commission needs to adopt measurement and public reporting requirements as part of its rules and policies.

The industry has long been able to measure performance by the number of complaints or the number of tracebacks leading to a specific service provider. However, technology exists today that monitors a service provider's traffic associated with the Direct Inward Dial telephone numbers ("DIDs")

the carrier "owns" and then detects illegal activity on those DIDs. This information, in turn, can be used to score the performance for specific DIDs, i.e., the percentage of calls from a service provider's DIDs that are robocalls. Information can be used to explore how many spoofed robocall campaigns are passing through a service provider's network. Also, the same information can be used in conjunction with a service provider's Call Detail Records ("CDRs") to locate instances of scam campaigns and to determine which times of day its network is being used for spoofed traffic.

Measurement and reporting scores by service providers to the public can enhance competition. Service providers with relatively clean performance may gain customers, while companies with poor scores will have an extremely strong incentive to improve or face business failure. Consumers will be able to make more informed choices, picking providers that have better performance suppressing robocalls. Certainly, mandatory measurement and reporting of scores is in the public interest.

V. Conclusion

For the reasons explained above, YouMail urges the Commission to require all carriers to take effective action against robocalls now. All service providers, including those that obtain an extension for full compliance with STIR/SHAKEN, must implement effective and efficient robocall mitigation programs and have their performance measured and reported. Technology exists today that will enable service providers to identify bad traffic and its source quickly, as soon as the capture of one call, and, after investigating the details, work to shut down these sources in days, not weeks or months.

Respectfully submitted,
YouMail, Inc.

By /s/ Robert H. Jackson
Robert H. Jackson
Marashlian & Donahue, PLLC
1430 Spring Hill Road
Suite 310
Tysons, VA 22102
703-714-1300
rhj@commlawgroup.com

October 16, 2020