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 YOUMAIL, INC.

YouMail, Inc. ("YouMail"),[1] through counsel, respectfully submits its reply comments in response to comments filed by various parties in reaction to the Federal Communications Commission's ("Commission" or "FCC") Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97.[2]

I. INTRODUCTION AND BACKGROUND

Multiple parties' comments focused on two key issues before the Commission. These are: 1) the use of analytics as the major tool to identify and block unwanted and illegal robocalls; and 2) protection from liability through an FCC-prescribed safe harbor for those entities that use such analytics in a reasonable manner. Indeed, YouMail recommended[3] that the Commission consider establishing, through the Commission's statutory authority to prescribe just and reasonable

[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 phone 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] *Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor*, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 and Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 21-105, 86 Fed. Reg. 59084 (October 26, 2021).

[3] Comments of YouMail at 10-13.

practices, pursuant to Section 205(a) of the Communications Act of 1934, as amended, an index-based safe harbor for gateway providers that provides protection against enforcement actions by the Commission, as well as from other regulatory agencies, state attorneys general and civil lawsuits.[4] In addition, YouMail urges the Commission to make clear exactly which Voice Service Provider ("VSP") has the obligation to block "bad traffic" and under what circumstances, to avoid inconsistent application of the FCC's rules and VSP confusion.

II. USE OF ANALYTICS

Multiple commentors urged the use of analytics to identify and block unwanted and illegal robocalls.[5] While those commenting generally see value in analytics, some, such as INCOMPAS, are also effectively concerned that, since analytics are not perfect, they can send false negatives for good calls and false positives for bad calls and can result in improper blocking.[6] At the microscopic level, INCOMPAS is right. No system of analytics is perfect. But that does not mean analytics cannot be extremely good for their users and the users' customers. It all depends on the sample size, the parameters measured and the underlying algorithms.[7]

YouMail's analytics are extremely good for identifying and enabling blocking of "bad traffic;" protecting consumers from unwanted and illegal calls; and guarding the reputations of businesses, nonprofits and other entities from being associated with robocalls. And this statement is not mere polish applied by YouMail's marketing department. Rather, it is supported by facts.

[4] 47 U.S.C. § 205(a).

[5] Comments of Transaction Network Service ("TNS") at 1-2; Comments of Twilio at 6; Comments of iBASIS at 10-11; Comments of INCOMPAS at 8, 10-11, 13-14; Comments of Comcast at 8-9;

[6] Comments of INCOMPAS at 10-11.

[7] As more and more traffic informs analytics, they will be more accurate and cause fewer "good" calls to be blocked. While every VSP should minimize blocking "good calls," blocking more and more "bad" calls best serves the public interest.

The US Telecom Industry Traceback Group ("ITG"), which is the "single consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls"[8] uses YouMail as a key supplier for robocall analytics.[9] So does one of US Telecom's 2021 competitors for the single consortium selected by the FCC for robocall tracebacks.[10] Also, the Commission used the results of YouMail's analytics sent from the ITG as a source for evidence supporting a $225,000,000 forfeiture in March 2021.[11] The Commission has also used YouMail analytics results (provided by the ITG) to support "Cease and Desist" letters.[12] State attorneys general have also relied on YouMail analytics in their investigations and enforcement actions.

Why do YouMail's analytics provide good results? Unlike traditional analytics systems that rely on the behavior of calls from a given phone number to repeat continuously, YouMail operates as an "answering service" and bases its analytics on the audio presented by a call, which is irrefutable evidence of the intent of that call. If the audio on the call claims to be the Social Security Administration, for example, then YouMail links that call to all other such imposter calls using the same voice and tactics at that time. There is little room for error when the audio is captured and utilized to determine what a call's actual intent and contents are, irrespective of the number employed.

---

[8] *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, Report & Order, EB Docket No. 20-22, DA 21-1047 (rel. Aug. 25, 2021).

[9] FCC, "Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information," at 15 (rel. December 23, 2020).

[10] ZipDX, "Letter of Intent to serve as the Registered Industry Consortium (EB 20-22, DA 21-474)" (May 27, 2021). ("2019: The ZipDX Secure Traceback Portal, operating under the auspices of the ITG, hits its stride. The ITG's completely manual original system, based on a mailing list of participating providers, had been processing a handful of tracebacks each month. By May, the ZipDX portal was consistently processing over a hundred, with many completing in a day. ZipDX initiated and sponsored a relationship with YouMail, a consumer-facing robocall mitigation solution employing sophisticated analytics, to provide for traceback consistent, documented examples of unlawful robocalls.") *Id.*, at 7.

[11] *John A. Spiller*, Forfeiture Order, 36 FCC Rcd 6225, at nn.124, 125 (2021) (health insurance scam).

[12] *Prince Anand, PZ/Illum Telecommunications Telecommunications*, Letter, 2021 WL 4953715, at *1 (FCC October 21, 2021) (government agency imposters & credit card scams); *Christopher Ismail, Duratel LLC*, Letter, 2021 WL 4953712 (FCC October 21, 2021) (government agency imposters).

YouMail is a company dedicated to the fight against robocalling and restoring trust in, and value to, the nation's telecommunications system. YouMail's direct consumer solutions "answer over a billion live calls per year across well over 11 million registered users, powering America's most robust telephone sensor network in identifying and providing zero-hour protection against illegal calling campaigns and cyberattacks."[13]

Are analytics perfect according to a major user? Comcast correctly notes:

> All analytics-based call blocking is inherently reactive; in order to determine that a call pattern is likely illegal, a provider using reasonable analytics must first observe (and complete) a certain number of calls that trigger pattern-based blocking. In other words, even the best call analytics are likely to "allow" some number of bad actor calls to be completed.[14]

However, these comments are largely based upon the certain subset of analytics that rely primarily on repetitive behavior by originating numbers – numbers that make too many calls too quickly or to too many recipients. In fact, YouMail has been part of many investigations where these analytic systems have flagged and affected emergency alert calls sent out by local government agencies to reach their audience, that is, too many calls from a number not already known by that analytics system was viewed as a risk and affected.

YouMail, on the other hand, will answer the call and take a voicemail and transcribe that message to text. That process enables YouMail to understand that the first call from that number, of potentially hundreds to millions to come, has the intent to distribute a legitimate, valuable communication, and its understanding of the reputation of that originating number would not falsely flag it for blocking. If the content of the communication from that origination number instead matched the audio for known unlawful behavior, such as impersonation of a government agency, then YouMail analyzes the balance of that communication against the historical record of that number. If that number had previously for years made lawful pharmacy prescription reminder calls

[13] YouMail, "About YouMail," available online at https://www.youmail.com/home/corp/about (accessed December 15, 2021).

[14] Comments of Comcast at 8.

but today is mixed with government imposter calls, then YouMail knows the number has a mixed set of content at present and cannot be outright blocked as just an originating number to prevent the agency imposter calls without risk of also blocking the pharmacy calls.

Twilio calls for the Commission to "define reasonable analytics with more specificity."[15] iBASIS does too.[16] In recognition that both large VSPs and third-party providers have developed different types of analytics and to encourage further development and innovation, the Commission should not define "reasonable analytics" by their parameters, methodology or other limiting factors. Rather, the best approach is to set performance standards, while allowing the marketplace to work, thus, permitting VSPs and third-party vendors to meet the standards in multiple ways. Good analytics systems that meet VSP needs, including the requirement to follow FCC rules, will rise to the top. A functioning marketplace will enable VSPs to make the make-or-buy decision based on price and quality factors.

It is worth noting that simply having any type of analytics in order to "check the box" that analytics are in place is not sufficient to achieve the goal of reducing and preventing unlawful robocalls. The performance standards should also factor in that robocallers and the VSPs that enable them to "optimize" their calling patterns, in order to "not get caught." Rogues will avoid calling and remove from their dialing plans any end-users that represent higher risk to their operations in terms of discovery and subsequent pursuit by private, state or federal organizations. While YouMail believes it provides a market-leading solution, a provider that takes 100% of its traffic and subjects it to a broad end-point content discovery auditing process will know what those calls said as they reached consumers with the irrefutable evidence of unlawful activity and can measure its progress in reducing those communications to zero or near-zero as their key performance metric.

[15] Comments of Twilio at 6.

[16] Comments of iBASIS at 11.

III. A SAFE HARBOR IS NECESSARY TO INCENTIVIZE DESIRED CONDUCT FROM GATEWAY PROVIDERS

There is strong support among commenting parties[17] for the creation of a safe harbor for gateway providers that engage in desired behavior, *i.e.*, use proper analytics and sensible robocall mitigation plans to identify and shutdown bad traffic. Providing protection for gateway providers that follow the rules and make good efforts to use appropriate tools to stop both unwanted and illegal robocalls is not only logical but also serves the public interest as it incentivizes VSPs to improve their performance above the minimum regulatory requirements.

As recommended in YouMail's comments,[18] the Commission should create an "index-based" safe harbor that protects a high-performing gateway provider from all liability from both government agencies and private lawsuits when they "meet a very high level of performance on a consistent basis."[19] "Those are the providers that use both analytics and post-service KYC to allow only a very small number of robocalls, both illegal and unwanted, into the United States."[20] Such a powerful safe harbor would encourage companies to design better and better analytics, to make sound create/purchase decisions and to use analytics as a key tool in identifying and suppressing robocalls from foreign sources using North American Numbering Plan ("NANP") resources. Providers currently operate very quietly out of fear that any information that leaves their organization increases their liabilities.

IV. THE COMMISSION NEEDS TO CLARIFY WHICH VSPs ARE REQUIRED AND UNDER WHAT CIRCUMSTANCES TO BLOCK ROBOCALLLS THAT ARE HIGHLY LIKELY TO BE ILLEGAL

There is not consensus as to which VSPs, especially gateway providers, are supposed to block robocalls that, based on analytics and other mitigation measures, are "highly likely" to be

[17] *See, e.g.,* Comments of INCOMPAS at 12-14; Comments of T-Mobile at 6; Comments of i3forum at 6-7; Comments of TNS at 2-3.

[18] Comments of YouMail at 10-13.

[19] Id., at 11.

[20] *Id*.

illegal. For example, Comcast states that the Commission should "require gateway providers to take steps to know the upstream providers from which they directly receive traffic, and to take reasonable measures to prevent those providers from transmitting illegal traffic onto U.S. networks."[21] Comcast argues, "By extending call blocking and call authentication requirements to so-called 'gateway providers,' the Commission can reduce the flow of harmful foreign calls into our nation's voice networks."[22]

Yet, T-Mobile sees an imposition of blocking requirements on gateway providers as "problematic" and urges the Commission to reject such a requirement.[23] And some others are in the middle. For example, Twilio does not oppose a call blocking mandate on gateway providers.[24] iBASIS supports permitting, but not mandating, blocking.[25]

However the Commission decides this issue, it must not do so in a vacuum. It must be aware of other decisions, including a recent decision by one of the Commissions' own bureaus, that appear to be imposing a duty to block bad traffic on non-terminating carriers.

VSPs that enable the worst of the unlawful calls – those which commit fraud by impersonating brands or government agencies – need to be addressed by the Commission. This type of fraud (impersonation of legitimate and well-known brands or government agencies are part of the basis of the FTC's recently announced *ANPRM*.[26] These gateway providers, when they are using content-based analytics, can discover calls that "should not come this way" in their networks – while they believe they signed up a lawful call center, if they in fact find calls pretending to be a major US bank or government agency among that traffic, they can with their action prevent a large

[21] Comments of Comcast at 10 (footnote omitted).

[22] Comments of Comcast at1-2.

[23] Comments of T-Mobile at 5.

[24] Comments of Twilio at 6-7.

[25] Comment of iBASIS at i.

[26] *Trade Regulation Rule on Impersonation of Government and Businesses*, Advanced Notice of Proposed Rulemaking, FTC File No. R207000, 86 Fed. Reg. 72901 (2021) ("*ANPRM*")

portion of the US public from being affected by these calls, particularly as they are so close to the "head of the snake" in cutting off the traffic.

On December 7, 2021, the Pricing Policy Division ("PPD") of the Wireline Competition Bureau released an Order that rejected tariff revisions filed by Core Communications, Inc. ("Core"), a competitive local exchange carrier ("CLEC") that proposed changes to its tariff rules as to when disputed access charges must be paid by interexchange carriers ("IXCs").[27] While this was a tariff order and did not directly address foreign-traffic and robocalls, the tariff rejection as "unlawful on [its] face" and, as such, provides a level of confusion for VSPs. One of the reasons that the PPD used to justify its conclusion of law was that the tariff revisions "also unreasonably shift the responsibility for detecting and blocking fraudulent traffic onto its IXC customers in violation of the Commission's rules and orders."[28] Since the traffic at issue was toll free traffic, the IXCs are the terminating carriers that deliver toll free calls to an IXC's subscriber, *e.g.,* a reservation center. But the Bureau order puts responsibility for call blocking on an intermediate carrier.

The PPD, relying on a prior full-Commission tariff investigation order, also involving Core, stated that "'Core is in a better position' than the IXCs to which it sends the calls to 'identify the sources of and take steps to mitigate the impact of that traffic on downstream voice service providers.'"[29] The *Core Order* and the *Core Investigation Order* clearly put the responsibility for identifying and blocking "bad traffic" on upstream providers. Regardless of whether this is the correct place to put the burden to stop "bad traffic," the Commission's rules need to be consistent with each other. Inconsistent application of Commission rules, in particular as to the burden of

[27] *Core Communications, Inc., Tariff F.C.C. No. 3*, Order, WCB/Pricing File No. 21-02, Transmittal No. 22 (rel. December 7, 2021) ("*Core Order*")

[28] *Id*. at ¶ 6.

[29] *Id* at ¶ 12, *quoting Core Commc'ns, Inc., Tariff F.C.C. No. 3, Transmittal No. 17*, Memorandum Opinion & Order, WC Docket No. 21-191, FCC 21-109, at ¶ 40 (rel. October 7, 2021), ("*Core Investigation Order*"), petition for review filed, *CoreTel Delaware, Inc. v. FCC*, No. 21-3170 (3d Cir. Nov. 22, 2021).

identifying and blocking bad traffic, will create uncertainty and, inevitably result in more bad traffic slipping through to consumers.

The Commission must also address the potential inconsistency for responsibility of call-blocking obligations raised by INCOMPAS[30] in its discussion of the *Mey Case*.[31] That case seeks damages under the Telephone Consumer Protection Act ("TCPA") from intermediate carriers that allegedly transmitted calls "originating from non-standard telephone numbers."[32] Should plaintiff prevail, it will create legal precedent that intermediate providers have a duty to block "bad traffic," which contradicts the current rule[33] that focuses on the terminating carrier making the blocking decisions.

These examples provide clear and convincing reasons why the Commission must provide "bright line" guidance for which VSPs must block and under what circumstances. VSPs that follow the rules and best practices should be, indeed, must be, protected with a safe harbor. Moreover, the Commission should strongly consider YouMail's proposal for creating a performance-based safe harbor that offers those VSPs that meet or exceed a high-standard of compliance complete protection against public or private investigations, prosecutions or lawsuits. Failing to do so in a manner that leaves VSPs in a "damned if you do; damned if you don't" position that provides no incentive to meet or exceed high standard of compliance and will, for many, make the choice of quick profits for handing "bad traffic" a preferred approach. The good must be rewarded to best serve the public interest.

---

[30] Comments of INCOMPAS at 12-13.

[31] *Diana Mey v. All Access Telecom*, No. 5:19-CV-00237-JPB (N.D. W.Va., filed April 23, 2021) ("*Mey Case*").

[32] Comments of INCOMPAS at 12. INCOMPAS further notes that one of the defendants filed a motion for a primary jurisdiction referral to the FCC. The presiding judge denied the motion. *Id*. at n.21.

[33] 47 C.F.R. § 64.1200(k)(11). The rule makes no distinction between sent-paid and toll free calls.

V. CONCLUSION

As more fully explained in YouMail's comments, YouMail urges the Commission to draw a careful balance between allowing markets to function and stopping robocalls; adopt a "safe harbor" for VSPs properly addressing incoming foreign calls using NANP resources, using analytics and other robocall mitigation tools; and establish an index-based safe harbor for gateway providers. Finally, the Commission must clearly state a consistent rule as to which VSP must block calls and under what circumstances.

Respectfully submitted,
YouMail, Inc.

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

January 10, 2022