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 ENTERPRISE COMMUNICATIONS ADVOCACY COALITION

FIFTH FURTHER NOTICE OF PROPOSED RULEMAKING IN CG DOCKET NO. 17-59

FOURTH FURTHER NOTICE OF PROPOSED RULEMAKING IN WC DOCKET NO. 17-97

It is a truth universally acknowledged that an immense share of the illegal calls that consumers do not want to receive originate outside the United States. The calls originate abroad and are transmitted to the recipient through a confusing web of call centers, carriers, loosely regulated IP-based voice service providers, and gateway providers.

Those responsible for transmitting the illegal calls almost always transmit a US number in the caller ID field to increase answer rates. These calls must be delivered through a gateway and ultimately to the call recipient's terminating carrier without being blocked and, as the call originator hopes, without negative call labeling by the terminating carrier or its analytics provider.

Stakeholders are recognizing that callers originating legal and wanted calls have the same goals and face the same barriers as illegal callers. They engage in the same behaviors to increase the chances that their calls reach their intended recipients. This makes distinguishing between legal and illegal calls doubly difficult.

In regulating gateway providers, the Commission must ensure that it does not inadvertently erect obstacles that increase and impose costs and undue burdens on callers and carriers that are communicating lawfully.

The Enterprise Communications Advocacy Coalition ("ECAC") is a coalition of companies and organizations striving to ensure that lawful communications are not impeded by efforts to combat illegal robocalls. The ECAC strongly supports the Commission's efforts to extend the STIR/SHAKEN mandate and other obligations to mitigate illegal robocalls to gateway providers. But some of the proposals that require blocking and "know your customer" procedures will be both burdensome and ineffective. Finally, C-level attestation has a place in the call signing and traceback process.

I. Gateway Providers Should Not Be Required to Block

The Commission should not mandate call blocking by gateway providers. Although few commenters addressed this issue, requiring call blocking by gateway providers ultimately complicates the industry-wide efforts to address the problem. Other than blocking unallocated, unassigned, and invalid numbers, subjective blocking should be done by terminating carriers with customer consent and opt-in. Implementing a blocking requirement for gateway providers in the middle of a call path without clear objective criteria and a means for call originators to know who blocked calls and a redress for unjustified blocking is a major obstacle for legal call originators.

The Commission has proposed that gateway providers "*must* block calls that it reasonably determines, based on "reasonable analytics" that include consideration of caller ID authentication information where available, that calls are part of a call pattern that is highly likely to be illegal."[1]

This definition has four vague words: "highly," "likely," "illegal," and "reasonable." U.S. law has many different provisions defining the legality of a call. In fact, the Commission itself has struggled to define "illegal" robocall and to differentiate it from an "unwanted" robocall. Oftentimes, the distinction between legal and illegal is based on the consent of the call recipient, which is outside the purview of any carrier, let alone a gateway provider who has no direct knowledge of the call originator or recipient.

Further complicating the inherent difficulty in making a clear distinction between legal and illegal calls, the Commission does not create an objective standard around the words "highly," "likely," or "reasonable." What percentage of calls would be illegal to meet the "highly likely"

[1] *In Re Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 21-105, 45 (2021) (" (emphasis added). ("*Further Notice*").

standard? What types of analytics are reasonable? If a carrier hires one of the current analytics providers, is it protected from further inquiry into what that analytics provider does, how it makes those blocking decisions, and what factors go into those blocking decisions?

ECAC points out that many carriers engage in least-cost-routing practices that choose different routes and providers based on certain factors, including, but not limited to, destination and time of day. A caller may have calls blocked to certain phone numbers by an intermediate gateway provider that it didn't contract with that is using unknown blocking criteria. This caller can take advantage of no feedback mechanism to know who blocked the call and why and how to challenge that decision.[2]

Legal enterprise callers face enough challenges today in ensuring that their calls are delivered with accurate labeling to the Tier-1 carriers that terminate the vast majority of voice traffic. The challenges these callers face will increase exponentially when they are forced to engage with an unknown number of anonymous gateway providers using unknown criteria to block calls pursuant to a government mandate. T-Mobile correctly points out that blocking decisions are best made by the terminating carrier with input from the call recipient. A call recipient's blocking decision should not be frustrated by blocking requirements imposed on upstream providers that the call recipient cannot control or even be informed about. Blocking at the terminating carrier serves two functions. It allows the terminating carrier to best police its own network, but also empowers its customer to control which calls it receives or doesn't receive.

[2] The Commission is simultaneously engaged in creating procedures for transmitting call blocking information to the caller. *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Order on Reconsideration, Sixth Further Notice of Proposed Rulemaking, and Waiver Order (rel. Dec. 13, 2021). ECAC notes for the Commission that the requirements it is proposing here for gateway providers and the issues in the signaling requirements for call blocking are inextricably linked.

The ECAC supports call blocking in certain, defined circumstances. First, as noted above, call recipients should be empowered to work with their carrier to choose which calls to receive. Second, ECAC supports blocking of unallocated, unassigned, and invalid numbers. Third, ECAC supports blocking calls when the number is on a Do Not Originate List.

Spoofed calls using a legitimate entity's phone number are particularly harmful to both the entity being spoofed and the call recipient who may believe the call to be legitimately placed by the entity whose number and identity is being displayed to the recipient. The Commission's actions in November 2017 to allow blocking based on a Do Not Originate list is a workable measure to reduce fraudulent calls.[3] ECAC agrees with Somos' suggestion that if the Commission requires gateway providers to block based on the Do Not Originate list, the list should be broad and comprehensive.

II. If Gateway Providers Are Required to Block, the Commission Must Define the Reasonable Analytics to be Used to Make Such Important Decisions

In the *Further Notice*, the Commission questioned:

> Should we provide further guidance as to what constitutes "reasonable analytics" in this context? Other than in the *First Call Blocking Order*, we have declined to establish specific standards, both out of a concern that such standards will create a road map for bad actors seeking to avoid blocking and to allow flexibility in response to evolving threats. However, we want to ensure that a gateway provider has notice as to whether or not it is in compliance with our rules.

Id. at ¶ 70.

[3] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, CG Docket No. 17-59, FCC 17-151 (rel. Nov. 17, 2017).

ECAC agrees with the comments of Twilio, Inc.[4] and suggests emphatically that the Commission *must* provide guidance as to what constitutes "reasonable analytics" in this context. Without specific guidance from the Commission, the industry will be plagued by inconsistent interpretive standards governing call analytics.

Even more is at stake when state attorneys general strive to impose their own inconsistent – and frequently illogical – analytical methodologies and interpretations on gateway and other intermediate carriers as part of law enforcement investigations and enforcement actions. In doing so, *they* seek to define what "reasonable analytics" should include. Furthermore, attorneys general seem to implicitly, if not explicitly, suggest that calls that last less than 60 seconds are likely robocalls.[5] In doing so, they also suggest that ANIs that originate less than 10 calls in an analytical period must indicate random spoofing or "snow-shoeing."[6]

Gateway providers in particular, and intermediate carriers in general, cannot have arbitrary and inconsistent analytical standards applied to them. Whatever analytical framework is used to govern the analysis of when calls should be blocked appropriately must come from the Commission. Allowing any third party, including, but not limited to state attorneys general and law enforcement, to dictate appropriate analytics disregards the fact that the FCC has reserved to itself the sole authority to require intermediate voice providers to block an entire carrier's source

---

[4] *See In Re Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Comments of Twilio, Inc., 6 (Dec. 10, 2021) ("Twilio continues to be concerned that inconsistent and non-transparent analytics may result in mislabeled critical, lawful calls. All participants in the ecosystem would benefit from a better understanding of what constitutes "reasonable analytics," and if the Commission moves from permissive to mandatory call blocking in the case of gateway providers, it must take this opportunity to define reasonable analytics with more specificity.").

[5] Matt Fischer & and David Frankel, *Anatomy of a Robocall – Follow the Money*, 2021 NAAG Robocall Virtual Summit, 12 (2021), https://legalcallsonly.org/wp-content/uploads/NAAG2021Sep08.pdf.

[6] *Id*.

of traffic.[7] The alternative results in a chaotic environment where 50 state attorneys general, private plaintiffs and others can order intermediate providers to shut down an entire carriers' services, or sue them for damages *after* carrying traffic that that particular plaintiff would have stopped carrying sooner based on their private belief about the right blend of analytical tools. There needs to be a clear, single national standard, established via a public, prospective rulemaking proceeding conducted by the Commission.

III. Gateway Providers Cannot Know their Customer if the Customer is Defined as the Call Originator

Many commenters in this proceeding correctly pointed out that gateway providers are poorly situated to "know their customer" if the customer is defined as the entity that placed the call. As Twilio points out, at best gateway providers can "know" the entity that delivered the call to them. Many commenters correctly acknowledge that gateway providers have no basis to know the customer that may be several layers up in the call flow hierarchy—let alone whether that caller has the right to use the phone number it is signaling. ECAC agrees with these commenters. "Know

[7] *See In Re Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd. 7614, ¶ 37 (2020) ("a[n IVSP] may block calls from an upstream voice service provider that, when notified that it is carrying bad traffic by the [FCC], fails to effectively mitigate such traffic or fails to implement effective measures to prevent new and renewing customers from using its network to originate illegal calls.") (emphasis added); *see also In Re Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG-Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd. 15221, ¶ 28 (2020) (rejecting the ITG's request to have the authority to order mitigation on pain of carrier-level blocking: "Only the [FCC] should be able to provide notice of bad traffic and trigger [a blocking] requirement [because] if other entities provided notice in this context, it could lead to increased burdens and duplicative notice. . . . . We accordingly decline to authorize the Consortium to provide this notice"). As a practical matter, if carriers lack clear guidance on what "reasonable analytics" entail, it is clearly foreseeable that risk-averse carriers will simply suspend or terminate carrier services to carrier customers with traffic patterns that may not meet the highest standards, which would effectively undermine the Commission's decision in the Fourth Report and Order to reserve to itself the authority to order the carrier community to block an entire carrier's traffic.

your customer" obligations should play an important role in the STIR/SHAKEN environment, but that concept is logically limited to knowing those customers with a business relationship—not an obligation to know the details about every customer of any upstream carrier (and that carrier's customers) through multiple levels of interconnection.

IV. Proper Call Attestation Supports the Goals of STIR/SHAKEN

Finally, several commenters suggested that placing a C-level attestation by gateway providers is not worthwhile. This is wrong. C-level attestation has an important role in the STIR/SHAKEN environment.

The industry is approaching the A, B, and C attestation as though they were grades in high school where everyone is seeking an A. Callers and carriers are pushing the definitional limits of the categorizations in a misplaced notion that getting calls signed with an A will eliminate all problems with unjustified blocking and inaccurate labeling. Properly applied, the attestation categories should be based on knowledge supported by hard data. A C-level attestation is exactly what the drafters of STIR/SHAKEN intended to be applied to a gateway provider when it knows nothing more than where it received the call. This nugget of information is valuable for traceback efforts by law enforcement and industry to identify where the potentially bad traffic is entering U.S. networks. The entire STIR/SHAKEN ecosystem is now creating incentives for all players to enter into confusing and perhaps unjustified agreements to get an A attestation in circumstances where the creators of STIR/SHAKEN planned for B or C attestation. This is fueled by a misperception that an A results in a call being delivered without negative labeling, while B, C, and unlabeled calls are inevitably going to be blocked or receive a negative label. This is a gross misunderstanding of the goal of STIR/SHAKEN and how the analytics are currently evaluating calls and how those determinations and the call attestation are displayed to the call recipient.

V. The Commission Should Explore Less Comprehensive Blocking Parameters

The Commission's blocking strategy based upon "reasonable analytics" is untargeted, imprecise and overly broad. By its very nature, analytics *will* block lawful calls.

The Commission must keep in mind the distinction between *illegal* calls and *unwanted* calls. Not all *unwanted* calls are illegal. In fact, most likely are not. But, both illegal robocalls calls and legal unwanted calls appear similarly under an analytics-powered microscope: They are of short duration, compliant telemarketers initiate millions of calls transmitting a single ANI or transmit ANIs that are in the same area code as the call recipient. For these reasons, analytics cannot be used to distinguish between scam robocalls initiated by fraudsters, or unwanted calls initiated by compliant telemarketers.

ECAC finds the suggestion put forth by SipNav to be intriguing.[8] If the media IP address of the equipment used to initiate illegal robocalls is indeed attached to the illegal calls, it seems quite logical and simple to block the entry of calls containing the identified media IP address from entering the U.S. communications network. Focusing on this alternative blocking methodology filters out only the calls from *known* scammers without risking the blocking of legal calls. Furthermore, law enforcement should be able to leverage the transmitted media IP address to track-down the exact identity of the those responsible for the initiation of the illegal calls.

Respectfully Submitted,

ENTERPRISE COMMUNICATIONS ADVOCACY COALITION

By: /s Rebekah Johnson
Rebekah Johnson, Chairman

[8] *See Comments of SipNav LLC Regarding Commission's Fifth Notice of Proposed Rulemaking in CG Docket No. 17-59 and Fourth Further Notice of Proposed Rulemaking in WC Docket 17-97*, CG Docket No. 17-59 (2021)