

**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
)	

COMMENTS OF NUMERACLE

The Commission has taken commendable steps to help American consumers avoid the scourge of illegal robocalls. Both before and after the passage of the TRACED Act, the Commission has guided the development and implementation of STIR/SHAKEN. But the Commission’s work is not done. Illegal robocalls continue to be a nationwide problem, but at the same time callers making legal and wanted calls are encountering inaccurate blocking and labeling by carriers through their anti-robocall solutions.

It doesn’t have to be this way. The technology exists now for large volume call originators—whether it’s medical and prescription reminders, emergency alerts, financial notifications, or marketing and product support calls that customers have consented to receive—to have their identities vetted by a trusted entity. These callers then have the ability to have their identity transmitted in a secure manner by the originating carrier that begins the call routing path to the downstream recipient. These downstream carriers and the call recipients then will know not only what carrier originated the call but who the caller is as well. The carriers can use reliable information about the identity of the caller and the purpose of the call to inform their customers rather than guessing based on ever-changing phone numbers and calling patterns. The terminating carriers can then focus their anti-robocall efforts on callers that do not have an

identity or are unwilling to undergo the vetting process necessary to have their identity established.

I. End-to-End Call Verification Solves Many of the Questions the Commission Raises in the FNPRM

The FNPRM¹ has multiple questions about how to account for erroneous call blocking and labeling and how to implement safe harbors to protect carriers that will inevitably make mistakes. Such efforts are misplaced. Instead, the Commission should incentivize deployment of existing technologies that will minimize the need to account for errors.

Right now, the carriers make educated guesses as to the legality of calls and whether they are spam or not. The carriers make this determination number by number. If they see a suspicious calling pattern using a particular number, they block it. They augment their decisions with complaint data, honeypots, and other data sources that also are based on the individual telephone number. They do not see the entity behind the call that may be using multiple numbers. Numeracle has customers that use multiple numbers for identical types of outbound calls, and the carriers assign widely disparate ratings to identical calls from the same originator.

A better system tracks the identity of the call originator and not the phone numbers they use, which change over time for various reasons. The good callers are now mimicking the bad callers in cycling through numbers that have acquired negative reputations in the carriers' rating models. This makes accurate blocking and labeling more difficult, and it is also an inefficient use of limited numbering resources.

What if, instead, callers were known by their identity and not solely by the phone numbers they use? This technology already exists and is under consideration by ATIS as part of

¹ Advanced Methods to Target and Eliminate Unlawful Robocalls, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, WC Docket No. 17-59 (July 17, 2020) (“FNPRM”);

the STIR/SHAKEN standard. ATIS is calling this process “delegated certificates,” but perhaps a better name is end-to-end call verification. Each large-volume caller is vetted by a trusted entity to verify its identity associated with the authorized numbers used for outbound calling. Under the existing STIR/SHAKEN trust authority, the asserted information is extended in a secure manner to the originating voice service provider.²

Imagine a large retailer that makes calls for a wide variety of reasons, including delivery notifications, product recalls, service calls, sales inquiries, and many others. Under the current system—and even after STIR/SHAKEN is implemented—carriers have no ability to group all the different types of calls and numbers (that may come from a variety of carriers and sources) back to the entity responsible for the calls. But with end-to-end verification, carriers and consumers will know with certainty that “Retailer A” is making the call. Nobody is guessing anymore as to who made the call. Of course, even verified callers that strive to comply with TCPA and other laws may accidentally violate the strict rules. But with end-to-end call verification, law enforcement entities will know exactly whose door to knock on. The current process of tracing back only leads to the carrier, not the caller, and STIR/SHAKEN won't change that.

Using the end-to-end verification process would not be mandatory, but legal callers will have strong incentives to seek out originating carriers that will implement STIR/SHAKEN with end-to-end verification to associate their identity with outgoing calls. As STIR/SHAKEN becomes more widespread and eventually universal, callers without a verified identity will be suspect, and rightly so. Callers perpetuating scams will not want to provide the identifying information necessary to obtain end-to-end verification.

² Comments of Numeracle, WC Docket Nos. 17-97 and 20-67 (filed May 29, 2020), at 8.

Implementation of end-to-end call verification answers many of the commission's questions in the FNRPM or renders them moot.

The Commission asks whether blocking based on factors other than reasonable analytics incorporating caller ID verification should be permitted.³ With end-to-end call verification, the carriers are still making decisions to classify calls and display the information to consumers, but they are working with much more concrete and reliable information. The Commission's existing framework for blocking already incorporates the necessary tools without additional rulemaking except, as described below, to define reasonable analytics to include making use of free reliable data sources about the callers' identities.

The Commission also asks whether the safe harbor should be extended to blocking where the level of trust is incorrect. Again, end-to-end call verification minimizes the importance of this question because calls with this verification will have A-level attestation when signed within the standards of the SHAKEN framework. End-to-end call verification will minimize the importance of the ongoing debate about what types of calls should receive the highest level "A" attestation, and which should receive lower-level B and C attestations. All calls with a verified identity will receive an A-level attestation.

Third, in the long-term, end-to-end call verification will minimize but not eliminate the need for a redress process⁴ for erroneous blocking and labeling because legal callers with verified identities will be able to have their secure identities transmitted all the way to the call recipient. But in the meantime, disputes have arisen and will continue to arise as carriers will continue to incorrectly classify some calls. Even more troubling, as described below, is the refusal to accept verified caller data without payment. For now, the Commission should require

3 FNPRM para. 83.

4 *Id.* para 85.

carriers to respond to concerns about improper blocking within 24 hours and improper labeling within five business days.

II. Protecting Consumers from Calls From Unauthenticated Numbers

The TRACED Act requires the Commission to determine how to protect consumers from unwanted calls and texts from an unauthenticated number. As described above, the best way to protect consumers is to create a system where all or virtually all calls are signed and authenticated. Implementation of end-to-end call verification will incentivize callers and originating carriers to adopt STIR/SHAKEN rapidly so they can obtain the benefits of having their verified identities transmitted to the terminating carrier and ultimately the call recipient.

Callers making illegal and unwanted calls will not want to undertake the rigorous vetting process necessary for a verified identity. Anonymity is the illegal caller's greatest enabler. STIR/SHAKEN advances the goal of removing anonymity, but without end-to-end verification complete removal of caller anonymity will not fully achieved.

Callers making illegal calls will have a more difficult time finding a carrier willing to originate their calls. Even if they do find a willing carrier, the Commission has recently bolstered the authority and ability to block non-compliant carriers. Downstream carriers have more flexibility and authority to block upstream carriers that will not participate in STIR/SHAKEN and are willingly serving as gateways for illegal traffic. The end game that will finally minimize the quantity of illegal calls is an ecosystem where illegal callers cannot find a carrier willing to accept their traffic, and if they do, provide a digital trail to lead law enforcement to their door.

The vetting process Numeracle envisions is not to establish the legality of calls. It's to establish who is making the call. The vetting entity has no need to deeply dive into the particulars of the call, but rather who is making the call so we can send the lawman after the bad guys.

Nevertheless, the vetting process itself provides useful information about the legality of calls. Numeracle has identified, verified, and vetted its customers. As part of the vetting process, Numeracle evaluates its customers policies and procedures for regulatory compliance. And while Numeracle is not in the business of evaluating and guaranteeing the legality of its customers calls, thus far none of Numeracle's customers has been determined to be making illegal calls. Numeracle has refused to accept as clients entities that will not provide the required information needed to verify their identities.

III. Carriers Must Incorporate Free Call Registry Information to Obtain Safe Harbor Protection Under “Reasonable Analytics” Standard

No safe harbor should apply if a carrier does not take in accurate, freely available sources of information about verified callers. For more than two years, Numeracle has been working with callers making legal and wanted calls, verifying their identity, and registering their numbers with the analytics providers selected by the major carriers to provide its reasonable analytics. Carriers should not be permitted to invoke safe harbor protections without ingesting this and other similar vetted data sources. Failure to do so is unreasonable and therefore, analytics without these data sources does not meet the “reasonable analytics” standard necessary to invoke safe harbor protections.

Numeracle provides carriers and their analytics solution provider with verified caller information to assist in making determinations about how to classify calls. While this process has not been without its difficulties, for the most part Numeracle has been successful in ensuring that legal calls made by its customers are not blocked or labeled as scams. Unfortunately, as of late, one major carrier has converted the registration process to a pay to play. We are hopeful the carrier will recognize the value in receiving free information to improve the accuracy of its call protection product.

Numeracle recognizes that it is difficult to craft rules describing exactly what data sources a carrier must utilize in order for its analytics process to be classified as reasonable, but at a bare minimum, these decision makers should be required to accept information from entities with an established track record performing these services, which includes not only Numeracle but its competitors providing similar services. Failure to consider these important and reliable data sources is inherently unreasonable, and safe harbor protections should not apply.

IV. Commission Should Keep Focus on All Types of Emergency Calls

The Commission is rightly concerned about the effects of anti-robocall efforts on emergency calls, but the Commission's focus on 911 inbound calls and callbacks misses the larger problem. Numeracle has not seen that calls to 911 are being blocked. Nor that return calls from PSAPs and 911 call centers are being blocked or labeled. Thus far, their calling patterns do not seem to trigger negative treatment by analytics. The actual existing problem is large-scale outbound emergency calls, such as hurricane alerts and public-health notices related to COVID. Numeracle has created a free service for government entities to register their phone numbers to lessen the risk of inaccurate and dangerous mistreatment of these calls,⁵ but the long-term solution is to have end-to-end verification so that the carriers do not have to continue their guessing game as to the source and purpose of calls.

V. Numeracle Supports A Traceback Mandate

Numeracle supports the Commission's proposal to make participation in the traceback process mandatory. Although eventually universal implementation of STIR/SHAKEN will make traceback less important to the coalition battling illegal robocalls, for the time being, the traceback process implemented by USTelecom has been effective in tracing back many illegal

⁵ www.criticalcallsregistry.com

calling campaigns to the originating provider, putting a stop to those calls, and helping law enforcement agencies target the illegal callers.

VI. Numeracle Opposes Requirements that Terminating Carriers Provide Blocked Call Information to Subscribers

While well intentioned, the Commission's proposal to require terminating carriers to provide a list of blocked calls to their customers is unlikely to be of much benefit. Numeracle recognizes that consumers have a legitimate interest in seeing what calls their carrier is blocking on their behalf, but Numeracle also recognizes that the IT burdens of implementing such a system may be significant. In a calling ecosystem with widespread adoption of STIR/SHAKEN and end-to-end call verification signing, the number of false positives that are blocked in error should diminish to a trivial amount.

VII. Know Your Customer Practices Can Help Fight Illegal Robocalls

Numeracle introduced the concept of “know your customer” years ago to remove anonymity in support of STIR/SHAKEN caller authentication. In order to authenticate a caller, one must know who the caller is.

Numeracle continues to support an obligation that carriers originating large volumes of automated calls should have sufficient information about the caller to support inquiries from downstream carriers and traceback efforts to support law enforcement efforts. This vetting process could be burdensome for smaller carriers. But the vetting does not have to be performed by the carriers themselves. As described above, trusted vetting entities can do the work for the carriers then provide a verified identity so that these customers can take their calls to any carrier supporting this technology, thereby achieving the universal goal of knowing who originates a call and how to contact them when there are concerns about the legality of the calls.

Respectfully submitted,

NUMERACLE

A handwritten signature in black ink, appearing to read "Rebekah Johnson", with a long horizontal flourish extending to the right.

Rebekah Johnson
Founder and CEO

August 31, 2020