Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls	)	
	)	

<u>VERIZON'S COMMENTS ON PUBLIC NOTICE</u>

William H. Johnson
    Of Counsel

Gregory M. Romano
Christopher D. Oatway
1300 I Street, N.W.
Suite 400 West
Washington, DC 20005
(202) 515-2400

Attorneys for Verizon
and Verizon Wireless

July 20, 2018

TABLE OF CONTENTS

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls	)	
	)	

VERIZON'S COMMENTS ON PUBLIC NOTICE

No single or simple answer exists to the complex robocall problem, but Verizon is committed to addressing it on every available front. Technology is part of the answer, so Verizon offers industry-leading blocking and labeling tools to its wireline and wireless customers, deploys anti-spoofing technologies, and leverages its best-in-class feedback website to rapidly identify and reverse any incorrect blocking or labeling. Another important piece of the puzzle involving multiple stakeholders is to staunch the flow of illegal robocalls at the source. The Commission should seize several opportunities to shift robocall mitigation into a higher gear to protect consumers from unwanted and harassing calls.

Industry efforts to root out the bad actors who make illegal calls continue to face collectivity challenges. Verizon and a handful of other responsible communications providers actively work to shut down illegal robocallers, while many others are disinterested in solving the problem or even look the other way when accepting traffic they know or should know is illegal. As a result, the flood of illegal robocalls shows no sign of stopping. And because of the ease with which bad actors can engage in Caller ID spoofing, only a subset of robocalls can be stopped by blocking filters on the terminating side. The Commission can help by working with industry to stop robocalls at the source. It should promote good faith cooperation by all voice providers with industry traceback efforts; take enforcement action against service providers who

routinely ignore evidence they are providing high-volume services to clearly illegal robocallers; and consider requiring voice providers who fail to take meaningful action to stop illegal traffic to file reports with the Commission on their customers' traffic metrics so the Commission can identify which voice providers may be catering to illegal robocallers.

Restoring trust in voice calls will not only protect consumers but also benefit the entire ecosystem, including legitimate enterprises that use automated technology to communicate efficiently with their customers for pro-consumer purposes. Continued frustration with unwanted and illegal robocalls causes consumers to avoid calls from unknown sources, which appears to be reducing the contact rates of legitimate enterprises who follow the rules while using autodialers to contact their customers.

I.   NEW TECHNOLOGIES AND TOOLS BENEFIT CONSUMERS BUT BAD ACTORS EVOLVE TO TRY TO BYPASS THEM.

A. Consumers Benefit from the Large and Growing Number of Options They Have for Controlling What Calls Ring on Their Devices.

Verizon offers its customers ever-more robust options for avoiding unwanted and illegal robocalls. For wireless customers, our Caller Name ID service offers blocking as well as labeling functionality on most smartphones. It includes an innovative "risk meter" that classifies each incoming call, and permits subscribers to either make their own decisions on whether to answer likely-unwanted calls, or to select the category/categories of calls that they want to be automatically filtered and sent to voicemail.[1] Our wireline customers benefit from our Spam Alerts service, which helps customers protect themselves from potentially malicious

---

[1] *See* https://www.verizonwireless.com/support/caller-name-id-faqs/.

robocalls.[2] That service is available at no additional charge to all landline voice customers with Caller ID, whether they use fiber or copper facilities. Customers' Caller ID displays show "SPAM?" before a caller's name if the calling number matches certain criteria designed to identify likely spam.

To help refine our blocking and labeling tools, and to care for the concerns of legal robocallers whose calls theoretically could be incorrectly identified as spam, Verizon has created the industry-leading feedback website.[3] That website invites legitimate calling parties and consumers to tell us about calls that they believe are incorrectly labeled—both calls incorrectly identified as spam and ones that should have been identified as spam but were not. It also permits calling parties to simply tell us about their operations (such as the numbers they use and the nature of their calling campaigns), even if they are not aware of any issues with our labeling or blocking, so that the third-party vendor that analyzes traffic for Verizon's blocking/labeling tools can take that information into account. Verizon also educates calling parties about "best practices" and about the sorts of calling activities that can result in their calls being identified as spam, so that they have the opportunity to adjust their operations in order to avoid becoming caught up in Verizon's or other parties' blocking or labeling tools.[4]

Verizon's blocking and labeling tools provide concrete benefits to our customers, who demand relief from illegal robocalls. And we support our customers' right to use the large and growing array of options third parties make available to stop robocalls. One option for many

---

[2] *See* http://www.verizon.com/about/news/block-spam-robocalls-with-verizon-new-tool.

[3] *See* www.Voicespamfeedback.com and www.spamalerts.verizon.com

[4] Those materials are available at https://www.voicespamfeedback.com/vsf/bestPractices and are reproduced as Exhibit A.

wireline customers is Nomorobo, which provides a free blocking service using the simultaneous ring feature that is available to customers who receive Voice over Internet Protocol (VoIP) service. Verizon makes sure its Fios Digital Voice customers, who receive the simultaneous ring feature for free, are aware of the Nomorobo option, and we have worked with Nomorobo to implement a "one click" feature to enable our customers to efficiently sign up with that service if they choose to do so. Verizon also makes sure that our wireline customers (on both copper and fiber facilities) are aware of the various devices that they can use to block robocalls, such as the CPR Call Blocker.[5] And our wireless customers have the option, if they choose not to use our Caller Name ID service, to download an array of competing third-party blocking and labeling apps from their app stores.[6]

The variety of robocall blocking/labeling options available to consumers empowers them to choose the tool that best suits their individual needs. This Commission and the Federal Trade Commission (FTC) have correctly focused on raising customer awareness of their options, including with the successful Stop Illegal Robocalls Expo in April 2018.[7] Recognizing that consumer education may be particularly beneficial if provided at the moment consumers are complaining about robocalls, Verizon has developed a package of consumer education materials to help consumer-facing personnel, such as staffers at consumer protection agencies or in constituent-services offices, effectively counsel consumers about robocalls. Counselors are encouraged to first ask questions to elicit the nature of the consumer's service and facility (e.g.,

---

[5] *See* https://www.verizon.com/support/residential/homephone/service-equipment/call-blocking-device.

[6] *See* https://www.ctia.org/consumer-resources/how-to-stop-robocalls.

[7] *See* https://www.fcc.gov/news-events/events/2018/04/stop-illegal-robocalls-expo.

smartphone, wireline VoIP, wireline copper), and then the talking points have a "decision tree"
that counselors can follow to tailor their advice to each customer's particular technology
platform and his or her needs. The package includes different educational brochures to be
mailed or emailed consumers based on what makes sense for each one.

B. Bad Actors Evolve Their Techniques to Bypass Blocking and Filtering Tools.

Unfortunately, Verizon's statistical analysis confirms what consumers already know: bad
actors are spoofing extensively to bypass blocking and labeling tools. "Neighbor spoofing,"
which typically involves sending calls with the same (or a similar) NPA/NXX as the called party
while randomizing the last few digits with every call, has exploded. Verizon estimates that for
its wireline and wireless networks between March 2017 and August 2017, neighborhood calling
patterns increased by approximately eightfold. Then, in September 2017, the volume of calls
showing a neighborhood pattern fell by about 50%, and subsequently have been rising again.[8]
Bad actors, possibly to avoid blocking algorithms that may be set to detect the spoofing of the
first six digits (i.e., the entire NPA/NXX), also increasingly have been altering their spoofing to
include only the first three, four, or five digits.

The result is that, although blocking and labeling tools deployed at the terminating edge
of networks can stop many unwanted and illegal robocalls, the flood is not ebbing. Based on the
percentage of calls identified by Verizon's Caller Name ID and Spam Alerts service during April
2018, and extrapolating to the entire U.S. population, Verizon estimates the total number of spam
robocalls nationwide to have been between 3.7 and 4 billion that month. And that is a

---

[8] That volatility suggests that a relatively small number of callers may be responsible for a
substantial percentage of these robocalls. That suggests that the opportunities discussed in
Section II for industry and government to more effectively identify and shut down illegal
robocallers could materially reduce the total volume of illegal robocalls.

conservative approach that may understate the scope of the problem because it takes into account only calls that trigger strong spam warnings, but not milder spam calls. These identified calls were a 13% increase since January 2018, which may in part be a reaction of the bad actors to increased enforcements by both network providers and user tools.

C. Verizon and Some Others Are Implementing Technological Solutions to Strike Back Against Spoofing.

Verizon is committed to addressing the spoofing problem with technology, including implementing the STIR/SHAKEN standard. We expect to achieve initial operational capability with STIR/SHAKEN this year, with the bulk of production coming on line in 2019. But here too industry faces a collectivity problem: the promise of STIR/SHAKEN can be achieved only once a substantial portion of the ecosystem has deployed the standard because the "signatures" that are sent with calls can only be authenticated by the terminating voice providers if each provider in the call path has implemented STIR/SHAKEN. Any calls not originated by a provider that signs calls using the STIR/SHAKEN protocol, or any calls transiting any non-STIR/SHAKEN providers, cannot be authenticated.

While the widespread adoption of STIR/SHAKEN may occur organically via market forces, the Commission is correctly keeping an eye on providers' implementation plans. It should stand ready to step in if substantial portions of the ecosystem fail to promptly implement STIR/SHAKEN. Because of the uncertainties about the timing and scope of many voice providers' STIR/SHAKEN deployments, however, and the fact that even a fully-deployed STIR/SHAKEN standard will not be a panacea, the Commission and industry should not over-rely on its promise. Instead, we should complement STIR/SHAKEN with other techniques for addressing the spoofing problem. Specifically, as discussed below, now is the time to seize opportunities to more aggressively stymie illegal robocallers.

II. THERE ARE MULTIPLE WAYS TO DO MORE TO ROOT OUT ILLEGAL ROBOCALLERS AND TO PREVENT VOICE PROVIDERS FROM ACCEPTING THEIR TRAFFIC.

A. All Voice Providers Should Participate in Industry Traceback Efforts.

As a founding member of USTelecom's Industry Traceback Group, Verizon has for years been formally committed to two simple, commonsense principles that all voice providers should follow. First, Verizon has agreed to promptly process traceback requests, which means that if presented with information from the traceback group that suspicious high-volume traffic was detected coming from one of our networks, we will investigate the traffic and provide the traceback administrator with the identity of the upstream provider(s) that sent Verizon the traffic.[9] Second, if the source of the suspicious robocalls is a call center or enterprise that is a Verizon customer, we agree to shut down that customer unless it justifies the legality of its traffic.[10]

If every voice provider in the call path embraced those two simple principles, the number of illegal robocalls would be reduced, both because we could identify and shut down more illegal robocall campaigns and because we would be able to refer a larger number of attractive prosecution targets to enforcement agencies. But unfortunately it is common for traceback investigations to dead-end when an upstream provider refuses to participate. There is no valid justification for those companies' intransigence. Our experience in the traceback group has confirmed that it typically is not difficult to determine where suspicious calls are coming from.

---

[9] Verizon's traceback team fields requests on a 24/7 basis, although that is not required by USTelecom's rules for its Traceback Group. Some smaller providers who participate in traceback generally only undertake traceback requests during regular business hours.

[10] In practice, no USTelecom traceback has led to a Verizon retail customer.

To the contrary, it ordinarily can be done relatively quickly and easily, once some systems work

is done to facilitate the process.[11] Given the compelling consumer need and the fact that

voluntary efforts are falling short, the Commission should promote ubiquitous participation in

industry-led tracebacks.

B. Consumers Would Benefit from Stronger Partnerships Between the Experts at the FCC and FTC and the Criminal Law Enforcement Agencies with Jurisdiction to Prosecute Fraud.

This Commission and the FTC have teams of sophisticated enforcers doing excellent

work rooting out robocallers who violate the Telephone Consumer Protection Act (TCPA)[12] and

the Truth in Caller ID Act.[13] But the civil actions they can bring do not have the same impact as

putting bad actors in jail, which is the right penalty for robocallers who commit criminal fraud.

Criminal law enforcement agencies' expertise in following money flows and bringing criminal

charges against fraudsters would be an invaluable complement to this Commission's and the

FTC's expertise identifying and tracing back robocall-related misconduct.

To the extent there is any doubt about the ability of motivated criminal law enforcement

agencies to meaningfully combat fraudulent robocalls, the Treasury's Inspector General for Tax

Administration (TIGTA) offers an excellent case study. TIGTA devotes substantial resources to

---

[11] There are, of course, sometimes valid constraints that render tracing back certain traffic impractical or in some cases even impossible. Detailed best practices are under development, but in the near-term the expectation for voice providers is simply to commit to undertake reasonable efforts to identify the source of suspicious traffic and to report that information to the traceback administrator.

[12] Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, *codified at* 47 U.S.C. § 227.

[13] Truth in Caller ID Act of 2009, Public L. No. 111–331, *codified at* 47 U.S.C. § 227(e).

combat scams where bad actors impersonate Internal Revenue Service personnel, with impressive results. It has investigated, arrested, indicted, and prosecuted dozens of individuals and has shut down multiple call centers responsible for billions of robocalls and tens of millions of dollars of fraud.[14]

But TIGTA does not investigate crimes that are not tax-related, so consumers need other criminal law enforcement agencies to step in. If criminal enforcement agencies join this Commission and the FTC to conduct robocall fraud investigations, such joint enforcement—especially if coupled with stronger private sector traceback activity—could reduce the number of illegal robocalls American consumers receive.

C. Industry and the Commission Can Use Metrics Consistent with Illegal Robocalling to Help Root Out Complicit Voice Providers.

1. Verizon Has Developed Know-Your-Customer Procedures Based on Readily-Calculated Traffic Metrics.

There is a growing industry consensus that, in addition to tracing back suspicious traffic on an *ad hoc* basis, voice providers should also be taking measures to avoid providing high-volume calling services to illegal robocallers in the first place. To that end, Verizon's know-your-customer procedure begins with running daily analytics on all customers served on Internet Protocol platforms (both wholesale and retail customers) to proactively look for patterns that are consistent with illegal robocalling activity. Then we take a closer look at any customers that trigger particular thresholds.

---

[14] *See* Testimony of Timothy P. Camus, Deputy Inspector General for Investigations, Treasury Inspector General for Tax Administration, "Stopping Senior Scams: Developments in Financial Fraud Affecting Seniors," Senate Special Committee on Aging, at 3 (115th Cong. Feb. 15, 2017), https://www.treasury.gov/tigta/congress/congress_02152017.pdf.

Verizon's first step is to create, for each retail and wholesale customer, a report Verizon calls a "Robo Score." We calculate that score using standard data elements that all voice providers have in their systems: each customer's unanswered rate (including calls that calling parties choose not to answer, calls the caller cancels, and calls to unassigned numbers) and its average call duration. The unanswered rate is an indicator of how willing call recipients are to pick up their phone for a caller, as well as the extent to which a caller may be "carpet-bombing" large swaths of numbers that are not even assigned to anyone. The average call duration is an indicator of how long call recipients stay on the line when they do answer the call. We combine the unanswered rate and call duration into a single score, with higher scores representing behavior that is more consistent with (but is not necessarily indicative of) patterns known to be associated with illegal robocalling.[15]

After calculating Robo Scores for all customers, we look more closely at those with the highest ones to determine whether they are complying with their contractual obligations to not engage in illegal conduct. For those customers, we run additional analytics:

- Volume. Number of calls in a 24 hour period.

- Velocity. How many calls the customer makes per second.

- Neighbor-ness Score. This is a proxy for possible neighbor spoofing.

  o It identifies all calls and compares the calling and called numbers for 6-digit matching (NPA-NXX-_ _ _ _), 5-digit matching (NPA-NX_-_ _ _ _), 4-digit matching (NPA-N_ _-_ _ _ _), and 3-digit matching (NPA-_ _ _ - _ _ _ _).
  o As discussed above, neighbor spoofing can be used to can hide the caller's identity. It can also be used to potentially increase its answer rate because some consumers may be more likely to answer if they believe the call is from a neighbor.

---

[15] *See*, *e.g.*, ZipDX Ex Parte Comments, CG Docket No. 17-59, at 11-14 (October 26, 2017).

- Spam Score. This is derived from the scoring that Verizon's third party analytics provider supplies for Verizon's Caller Name ID and Spam Alerts. It rates calls from -4 (the "worst of the worst") to -1 (the mildest spam traffic).

We use these additional reports to further evaluate those customers that initially triggered high Robo Scores. For those customers whose traffic is still determined to be potentially of concern after reviewing these additional metrics, we engage with them directly and require them to justify the legality of their traffic.

Importantly, we are seeking *only* to identify conduct that is clearly illegal and thus a violation of the customers' terms of service. We are *not* seeking to determine whether legitimate enterprise customers' TCPA compliance programs are valid. Second-guessing legitimate customers' compliance with the TCPA would not be an appropriate role for a voice provider, and it would be a virtually impossible undertaking given the TCPA's substantial nuances and complexities.

While Verizon's know-your-customer procedures are the industry's most sophisticated, other voice providers may have different and valid techniques for achieving the same results.[16] With no industry consensus regarding best practices, the Commission should not mandate at this time that voice providers must follow specific know-year-customer procedures. But the Commission could put all voice providers on notice that there will be consequences for not having *any* procedures, and should encourage similarly aggressive efforts by other providers. For example, the Enforcement Bureau could advise providers that it is an unreasonable practice for any voice provider to both (i) refuse to participate in good faith in industry traceback efforts

---

[16] Some voice providers simply do not provide high-volume services to any wholesale or retail customers. That likely obviates the need to undertake additional know-your-customer procedures. It is the voice providers that accept high-volume customer who need to have more detailed know-your-customer procedures in place.

and also (ii) not be able to document that it takes reasonable measures to avoid originating traffic that is illegal.

2. **Requiring Voice Providers Who Do Not Implement Effective Robocall Mitigation Measures to Report on Metrics Consistent With Handling Illegal Traffic Could Help the Commission Isolate Those Providers that Are Part of the Problem.**

Identifying traffic patterns consistent with illegal robocall activity should be part of the end-game on staunching illegal robocalls. Consumers have for too long endured the massive flood or robocalls originated by voice providers who know or should know that their customers are engaged in egregious conduct that is clearly illegal. While the Commission should rely on industry-driven robocall mitigation efforts, which continue to evolve and expand, it could backstop those efforts by targeting non-cooperating voice providers with robocall-related reporting requirements. For example, the Commission could require all voice providers who do not qualify for a safe harbor (e.g., participating in tracebacks, following effective know-your-customer procedures) to file reports containing their customers' Robo Score, Neighbor-ness Score, volume, and velocity metrics. Such reporting would not involve substantial burdens, and any perceived burden would be an incentive for providers s to take advantage of the safe harbor by helping to investigate and stop illegal robocalls.

One way to identify providers that may be accepting large amounts of illegal traffic would be to require voice providers to report the Robo Score, Neighbor-ness Score, and volume and velocity metrics described in the previous section. These reports are straightforward to calculate and are based on data that any IP-based voice provider can readily pull from its

systems.[17] For voice providers required to file reports, the Commission should consider

requiring then on a weekly basis. Each report should identify every customer (retail and

wholesale) whose Robo, Neighbor-ness, volume, and velocity metrics surpassed a particular

threshold. The reports should also include each voice provider's aggregate metrics (i.e., the

combination of all of its customers' metrics). The Commission staff could validate the accuracy

of filed reports by upstream providers by comparing their aggregate metrics with the reporting

from downstream providers about the traffic received from them; if the traffic reported by a

downstream provider has a higher Robo or Neighbor-ness score than what the upstream provider

reported to the Commission, that would constitute grounds to investigate the upstream provider

and penalize it if it falsified its report.[18]

These simple reporting requirements could form the basis for new enforcement activities,

and possibly new regulatory paradigms if industry efforts do not prove up to the task. For

example, the Enforcement Bureau's and FTC's staff could use these reports to improve their

understanding of robocall flows among voice providers at or near the source of illegal robocalls,

and to determine which providers merit enforcement scrutiny. Just as Verizon requires its

wholesale customers to justify their traffic if it triggers particular thresholds, the Commission

could issue subpoenas to providers with suspicious traffic demanding details with which to vet

---

[17] The Spam Score that Verizon uses is based on proprietary analysis by Verizon's vendor, so
not all voice providers can create identical reports on their customers' traffic. But there are
numerous other options for analyzing the extent to which a customer's traffic is triggering
consumer complaints. For example, some third party analytics providers make available
databases indicating what numbers they have classified as spam.

[18] Many downstream providers may be exempt from reporting requirements because they take
advantage of the safe harbor. The Commission could invite such non-obligated providers to
voluntarily file reports with the Commission so that it can vet the reports filed by upstream
providers and so that it can improve its understanding of robocall flows among providers.

their operations. And for voice providers that consistently fail to justify the legality of suspicious traffic, the Commission could contemplate additional measures, such as limiting the provider's ability to provide high-volume services.

CONCLUSION

Robocall mitigation techniques will need to continue to evolve as bad actors continue to find ways to hide their identities and to circumvent blocking and labeling tools. While technology like the STIR/SHAKEN authentication standard holds promise, it is also crucial that all stakeholders redouble efforts to address the problem at the source via robust traceback, enforcement, "know your customer" techniques, and reporting metrics.

Respectfully submitted,

_____

William H. Johnson
Of Counsel

Gregory M. Romano
Christopher D. Oatway
1300 I Street, N.W.
Suite 400 West
Washington, DC 20005
(202) 515-2400

*Attorneys for Verizon
and Verizon Wireless*

July 20, 2018

Exhibit A

verizon✓

Return to Verizon (https://www.verizon.com/)

Demand by consumers for protection from unwanted calls and spam has significantly increased over the years. Verizon provides tools that our customers can use to help decide whether or not to answer phone calls that may be unwanted, annoying, or fraudulent, and other third-party services are also available in the marketplace. Verizon is committed to helping consumers and calling parties navigate the robocalling landscape.

In addition to helping consumers, tools that restore trust in telephone calls will benefit legitimate businesses who want to communicate efficiently with their customers for pro-consumer purposes. Continued and growing frustration with unwanted and illegal robocalls can cause consumers to be less likely to answer calls, which in turn can reduce the contact rates of legitimate callers who follow the rules while using autodialers to contact their customers.

Calling parties can benefit from a greater knowledge of the constantly-evolving robocalling landscape, including an understanding of what calling practices can affect how their calls may be scored or categorized. Verizon's robocall analytics vendor, TNS/Cequint, considers a variety of factors when determining how to categorize or score calls being made to Verizon's customers. Those factors include feedback from consumers (such as complaints filed and crowd sourcing data) as well as information about calling patterns.

Here are some recommended industry best practices that are typically followed by legitimate callers who successfully avoid being categorized as spam (both by Verizon's spam protection services and from those provided by competitors):

Follow practices known to constitute good call center hygiene.

1. Provide a consistent, real, and user-dialable telephone number with every call you make. Calls with a calling party number that is invalid or not assigned to the caller are often associated with spam. You may want to consult your account representative at your service provider if you are unsure about this best practice.

2. Do not "random wardial" and do not call unassigned numbers frequently. Unreasonable answer and completion rates are often associated with spam.
3. Align the context and content of your calls to a specific traceable calling party number for the duration of that number's assignment to a particular campaign. Avoid using the same telephone number for multiple purposes. For example, using the same number for marketing, surveys, and support callbacks would typically increase the likelihood of being categorized as spam. It is recommended that numbers that are re-assigned for other purposes or allocated to other providers go through a 45-day waiting period.
4. Avoid unusual spikes in traffic volumes, and follow and document your expected and normative call pattern description (e.g. 10,000 caller per day).
5. Comply with "Do Not Call" lists and other TCPA requirements, and provide a number / contact information that called parties can use to prosecute or report any alleged violations of law.
6. Provide and document a consistent Calling Name profile that matches the context of the calls you are making and your callback information.

Use common sense to minimize the risk that consumers report your calls as spam or file complaints about you with government agencies.

1. Legitimate calling parties should never use abusive language, call too frequently, have perceptible delays in the quality or reliability of connection, or make unsolicited calls at odd hours.
2. Legitimate callers should always provide clear identification of the calling party, along with clear-and-easy opt-out directions.

For more information go to: https://www.verizon.com/support/residential/consumer-education/robocalls.htm (https://www.verizon.com/support/residential/consumer-education/robocalls.htm)

Feedback Form (/vsf/)