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
	)	
	)	

VERIZON'S COMMENTS ON FURTHER NOTICE

The *Report and Order*[1] exemplifies this Commission's laudable commitment to addressing the robocall problem. Verizon addresses this issue on multiple fronts, including offering wireline and wireless customers tools to avoid calls they may not want to take; deploying authentication technology to help address malicious spoofing (i.e., callers who transmit misleading calling party number information with calls); and working with law enforcement and industry traceback teams to root out the bad actors who continue to make illegal robocalls with impunity. In addition to helping consumers, these efforts to restore trust in voice calls will benefit legitimate enterprises who want to communicate efficiently with their customers for pro-consumer purposes. Indeed, continued frustration with unwanted and illegal robocalls can cause consumers to be less likely to answer calls from unknown sources, thereby reducing the contact rates of legitimate callers who follow the rules while using autodialers to contact their customers.

---

[1] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706 (2017) ("*Report and Order*" or "*Further Notice*").

The *Further Notice* tees up two important issues: (i) the potential harm that could befall legitimate callers from steps taken to combat robocalls and (ii) how to measure the effectiveness of the Commission's robocalling efforts.[2] On the first issue, although legitimate callers will benefit as efforts to address robocalls lead to consumers increasingly feeling they can answer their phones without being harassed or defrauded, the *Further Notice* raises a valid concern that legitimate callers potentially could be harmed if their calls are incorrectly blocked.[3] Efforts are underway to address that issue, and Verizon is contributing to best practices forums about mechanisms for legitimate callers to provide feedback about their calls. The Commission should encourage those efforts, especially given that the same feedback mechanisms being developed for opt-in blocking tools (ones third parties or service providers offer consumers who provide informed consent to the blocks) could potentially also be used by service providers who may choose to engage in the type of network-based blocking (i.e. on behalf of all consumers without individual opt-ins) contemplated in the *Report and Order*.

On the second issue, the Commission is right to ask about ways to measure the effectiveness of anti-robocalling efforts.[4] Although wireless and wireline consumers now benefit from increased access to blocking and labeling tools, this Commission's (and the Federal Trade Commission's) consumer complaint data show that robocall-related complaints are not stopping. So more still needs to be done. Data on robocall trends illustrate the challenges industry faces as bad actors increasingly find ways to bypass technologies that rely on lists of suspicious numbers. That means industry needs to improve existing tools, including by embracing anti-spoofing

---

[2] *Further Notice*, ¶¶ 57-59.
[3] *Id.*, ¶¶ 57-58.
[4] *Id.*, ¶ 59.

technology. It also highlights that no technological silver bullet will fix the robocall problem – so both industry and enforcement agencies need to redouble efforts to address the core problem by tracking down and prosecuting the bad actors who continue to break the law.

I. BLOCKING AND LABELING SERVICES HAVE AN IMPORTANT PLACE IN THE OVERALL ROBOCALL MITIGATION TOOLKIT.

A. All Stakeholders Benefit From Restoring Trust in Voice Calls.

After months of intensively examining the robocall problem, the Robocall Strike Force reported to the Commission in October 2016 that success will require continued action on multiple fronts (authentication, blocking, and enforcement), and emphasized the need to better educate consumers about how to protect themselves.[5] The interests of legitimate calling parties may have been lost in the urgency to find solutions. Given the explosion of robocall mitigation activity since then, the Commission is appropriately interested in caring for those legitimate callers.

Enterprises that use autodialers to make legitimate calls to their customers can find the complexity of the robocall mitigation landscape daunting, and some have expressed concerns that the misuse of the increasing number of blocking and labeling services may affect their calls.[6] To address those concerns, we need to increase transparency, educate calling parties about the implications of robocall mitigation tools, and take legitimate calling parties' concerns into account when refining ways to empower consumers to control what calls ring on their devices. But with these tweaks, the vigilant efforts to protect consumers from unwanted robocalls must

---

[5] *See* Industry Robocall Strike Force Report, at Executive Summary (Oct. 26, 2016), https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf ("Industry Robocall Strike Force Report").

[6] *See, e.g.*, *Ex Parte* Letter from Michelle Schuster of the Professional Association of Customer Engagement to Marlene Dortch (Nov. 9, 2017) ("PACE Ex Parte Letter").

continue. After all, the efforts underway to restore trust in voice calls, including efforts to offer consumers options to block calls they do not want to receive, will ultimately benefit legitimate calling parties because consumers are more likely to answer legitimate calls if they are bombarded with less spam.

B. Practices for Avoiding and Fixing False Positives Will Depend on Whether Blocking Is on an Opt-In or Non-Opt-In Basis.

The framework to address the risk of false positives (blocking a call that should not be blocked) depends on whether the call is blocked by a service provider on an across-the-board basis (i.e., the network-based blocking that is the subject of the *Report and Order*) or by a service that consumers opt into. Industry best practices forums should address both scenarios, but the practices will not be uniform. Any blocking that service providers may choose to do on a non-opt-in basis should be narrowly targeted, with strong procedures to promptly identify and reverse any blocks that affect legal calls. On the other hand, the Commission has made clear that consumers possess the ability to opt into blocking services that seek to protect them from "unwanted" calls, which may or may not be illegal.[7]

So not only are providers of opt-in blocking tools highly diverse (and the vast majority are not regulated by the Commission), but they have greater discretion to define what constitutes a "false positive" under their proprietary algorithms. While there is overlap in the issues relevant to addressing legitimate calling party interests in the opt-in and non-opt in contexts, such as potential web sites for fielding input from called parties, it is important not to conflate them.

---

[7] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Declaratory Ruling and Order, 30 FCC Rcd 7691, ¶¶ 151-62 (2015) ("*2015 TCPA Order*").

PACE, for example, says it is addressing "the Commission's recent activities to target and eliminate unlawful calls," but it appears more interested in the variety of opt-in blocking services that are relevant to the *2015 TCPA Order*.[8]

The distinction matters because sound policymaking requires understanding causality. PACE does not provide analysis about the impacts of different factors potentially affecting its members' contact rates, including opt-in blocking, non-opt-in blocking, labeling, and the probability that some consumers may simply be increasingly less likely to answer their phones. Verizon looks forward to working with all stakeholders to understand these issues well, and to incorporate the learning from PACE and others into the best practices discussions underway.

II. TRACKING DOWN AND PROSECUTING BAD ACTORS SHOULD BE THE CENTERPIECE OF ROBOCALL MITIGATION EFFORTS.

A. Data on Robocall Trends Illustrate Blocking's Limitations.

The Commission can look to its (and the Federal Trade Commission's) consumer complaint data as a general indicator of how efforts to combat robocalls are going. The continued flood of robocall-related complaints confirms what consumers already know, which is that robocallers are finding ways past the defenses currently being used. Just as bacteria evolve to avoid the body's antibodies, bad actors in the robocall space develop new strategies to evade detection and get their calls through to consumers. It is easy and cheap for bad actors to spoof legitimate or nonexistent numbers either for impersonation schemes or to bypass services that block or label suspicious calls based on the calling party number. Malicious spoofing creates

[8] *See* PACE Ex Parte Letter.

challenges for robocall mitigation services and can have unintended consequences for consumers.

Many consumers have noticed that they increasingly receive spam voice calls that appear to be from their own NPA/NXX. A year ago, relatively few illegal robocallers engaged in this practice, known as "neighbor spoofing." But Verizon estimates that, for its wireline and wireless networks between March 2017 and August 2017, neighborhood calling patterns increased by approximately eightfold, which likely indicates increased spoofing by calling parties.[9] In addition to potentially tricking the called consumer into thinking the call is local (and thereby potentially engendering more trust from some consumers), neighbor spoofing increases the likelihood that calls bypass blacklist-based blocking or labeling services because the robocallers can easily (and usually do) alter the last four digits of the calling party number with every call they make.

A different type of spoofing occurs when bad actors spoof legitimate customers' numbers, either to impersonate them or to bypass blacklists. When Verizon receives complaints from customers whose numbers have been spoofed by bad actors, the victims often complain about receiving large numbers of "reflective callbacks" from other consumers who call the legitimate (spoofed) number back. In some cases, there are so many callbacks that the spoofing victim requires a new telephone number. And as discussed below, identifying and shutting down the malicious callers is rarely a viable course of action.

---

[9] In September 2017, the volumes of the volumes of calls showing a neighborhood pattern fell by about 50%, and subsequently have been rising again. That volatility suggests that a relatively small number of callers may be responsible for a substantial percentage of these robocalls.

The ease with which bad actors can engage in such spoofing has policy implications,[10] and spoofing to bypass blacklists could become even more prevalent to the extent bad actors find themselves increasingly affected by blacklist-based blocking. That means robocall mitigation techniques will need to continue to evolve, including by incorporating anti-spoofing technology such as the STIR/SHAKEN authentication standard.[11] It also means, as discussed below, that industry and government should redouble efforts to address the problem at the source.

B. Current Enforcement and Traceback Efforts Need Strengthening.

This Commission and the Federal Trade Commission (FTC) have teams of sophisticated enforcers who are doing extraordinary work rooting out and bringing to justice illegal robocallers. And various service providers have banded together to identify bad actors by tracing back suspicious robocalls via USTelecom's Industry Traceback Group, of which Verizon is a founding member.[12] But while industry and government have made important strides, these efforts need to be strengthened if they are to have a material effect on the volume of illegal calls that reach consumers.

Although there is no valid excuse for any service provider to fail to cooperate with industry traceback efforts, tracebacks often dead-end when an upstream voice provider refuses to cooperate. And even though civil enforcement by this Commission and the FTC is robust, criminal enforcement agencies rarely devote the resources required to investigating and stopping

---

[10] *See* Verizon Comments, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, at 6-7 (Jan. 23, 2015).

[11] The Commission has correctly identified the need to ensure an effective governance regime for the industry-wide use of STIR/SHAKEN. *See Report and Order*, ¶ 4 n12; see also *Call Authentication Trust Anchor*, Notice of Inquiry, 32 FCC Rcd 5988 (2017).

[12] *See* Industry Robocall Strike Force Report; Ex Parte Letter, United States Telecom Association, CTIA, ATIS, ACTS - The App Association to FCC, CG Docket No. 17-59, at 19 (Apr. 28, 2017).

fraudulent robocall operations. They should. Their expertise in following money flows and bringing criminal charges against fraudsters would complement this Commission's and the FTC's expertise in identifying and tracing back robocall-related misconduct.

To the extent there is any doubt about the ability of sophisticated federal 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 combat scams where bad actors impersonate Internal Revenue Service personnel, with meaningful 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.[13] But TIGTA does not investigate other types of robocall-related crimes, so consumers need other criminal law enforcement agencies to step up and follow its lead.

If federal criminal enforcement agencies join this Commission to conduct robocall fraud investigations, such joint enforcement actions – especially if coupled with stronger private sector traceback activity – could materially reduce the number of illegal robocalls American consumers receive.

CONCLUSION

No single or simple answer exists to the complex, multi-faced robocall problem. It will require a sustained concerted effort by multiple stakeholders on multiple fronts. Part of the answer lies with offering consumers call blocking options, combined with deployment of anti-

---

[13] *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.

spoofing technology, which Verizon and others are undertaking in response to consumer demand. But the greatest imperative, especially pending the widespread deployment of Caller ID authentication technology, will be to more effectively track and shut down the bad actors who continue to spam consumers with impunity.

Respectfully submitted,

Christopher D. Oatway /s/

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

January 23, 2018