

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of

Advanced Methods to Target and Eliminate
Unlawful Robocalls

)
)
)
)

CG Docket No. 17-59

REPLY COMMENTS OF THIRTY-FIVE (35) STATE ATTORNEYS GENERAL

The undersigned State Attorneys General¹ (“State AGs”) submit these Reply Comments in response to the public notice issued by the Consumer and Governmental Affairs Bureau (“Bureau”), seeking to refresh the record on how the Federal Communications Commission (“FCC”) can further empower service providers to block illegal calls.² The State AGs have reviewed the comments submitted by voice service providers, consumer advocacy groups, consumers, private businesses, and other interested parties in the industry. In reply, the State AGs continue to support the FCC’s efforts to identify new ways to enable providers to block illegal calls before they ever reach consumers.

In the future, the State AGs encourage the FCC to adopt new rules authorizing voice service providers to block illegally spoofed³ calls beyond what is currently authorized in the 2017 Call Blocking Order.⁴ Likewise, we encourage all providers to use all available tools to accurately identify illegal calls, including continually monitoring call traffic patterns⁵ to develop and refine criteria for identifying such calls; and continually updating and developing technology in the event current systems and solutions become obsolete. In addition, providers who offer blocking or labeling tools should distribute to consumers – especially seniors – adequate information about the availability of these tools, how they function, and what effect they can have.

The State AGs intend to continue our fight against illegal robocalls and abusive calling practices on the front lines – by providing public education and outreach, receiving and responding to individual consumer complaints, and taking appropriate enforcement action when possible. We

will continue to do everything possible to track down and hold accountable those who engage in illegal calling practices. The State AGs recognize that no single tool or method will solve this serious consumer problem. Therefore, we are committed to continuing our multi-pronged attack of working closely with all interested parties, including our federal counterparts and members of the telecommunications industry.

A. Law Enforcement Alone Will Not Solve the Robocall Problem

Our respective Consumer Protection Offices receive and respond to tens of thousands of consumer complaints each year concerning the disruptive and abusive nature of these calls.⁶ We then attempt to identify and target potential wrongdoers. However, it is common for our efforts to be frustrated, as these types of calls travel through a maze of smaller providers. If the calling party is found at all, he or she is most often located overseas, making enforcement difficult. Due to the nature of this problem, investigations and enforcement actions cannot serve as the sole solution.

Virtually anyone can send millions of illegal robocalls and frustrate law enforcement with just a computer, inexpensive software (i.e., auto-dialer and spoofing programs), and an internet connection. Because “technology enables a cheap and scalable model,”⁷ illegal robocalls remain the “number one consumer complaint”⁸ for many of our Consumer Protection Offices, the FCC, and the Federal Trade Commission (“FTC”). Despite the 2017 Call Blocking Order, which increased providers’ ability to block illegally spoofed calls, the robocall problem appears to be getting worse.

B. The Impact to Consumers Is Increasingly Widespread and Deleterious

Based on available data, the number of illegal robocalls, and corresponding consumer complaints,⁹ increases every year. Last year, reports reflect that American landline and wireless subscribers received an estimated 30.5 billion illegal robocalls.¹⁰ This figure is up from the 2016 estimate of 29.3 billion illegal robocalls.¹¹ By the end of this year, the industry expects a 33%

increase, meaning spammers and scammers are going to disrupt our children's homework, our dinner, our relaxation time, and even our sleep, to the tune of over 40 billion illegal robocalls.¹²

Non-consensual robocalling in the telemarketing context is abusive and unlawful in and of itself.¹³ Many illegal robocallers, however, simply do not care about the law and have a more insidious agenda – casting a net of illegal robocalls to ensnare vulnerable victims in scams to steal money or sensitive, personal information. In fact, reports indicate, of the 4 billion illegal robocalls made just this past August, 1.8 billion were associated with a scam.¹⁴ Strikingly, criminals are estimated to have stolen 9.5 billion dollars from consumers through phone scams in 2017.¹⁵ If reports are accurate, scammers could potentially take even more in 2018.

Sadly, the fraud perpetrated by those employing illegal robocalls and other abusive calling practices falls heavily upon the shoulders of our respective senior populations. One year ago, on October 4, 2017, Pennsylvania Attorney General Josh Shapiro testified before the United States Special Committee on Aging with respect to protecting the elderly from financial exploitation.¹⁶ In his testimony before the Committee, and in a letter to the FCC sent shortly thereafter, Attorney General Shapiro highlighted the urgent need for the FCC to combat illegal robocalls, beginning with adopting rules allowing providers to block specific calls used in spoofing.¹⁷

C. Fraudsters Evolved to Evade the 2017 Call Blocking Order

On July 6, 2017, a bipartisan coalition of 30 state attorneys general submitted a comment, encouraging the FCC to adopt rules allowing providers to block calls from numbers on do-not-originate lists and from numbers that are invalid, unallocated, or unused.¹⁸ On November 17, 2017, the FCC released the 2017 Call Blocking Order, wherein it adopted rules allowing providers to block calls from these types of phone numbers, as they are used in spoofing. However, all concerned parties knew the new rules would not act as a 'cure-all' to the robocall epidemic. Soon after the 2017 Call Blocking Order was released, forty (40) state attorneys general formed the bipartisan, Robocall

Technologies Working Group in order to work together, and with providers, to understand the technological advancements, as well as the barriers, in combatting fraudsters' evolving methods.

One specific method which has evolved recently is a form of illegal spoofing called 'neighbor spoofing.'¹⁹ A neighbor-spoofed call will commonly appear on a consumer's caller ID with the same area code and local exchange as the consumer to increase the likelihood he/she will answer the call.²⁰ In addition, consumers have recently reported receiving calls where *their own phone numbers* appeared on their caller ID. A consumer who answered one such call reported the caller attempted to trick her by saying he was with the phone company and required personal information to verify the account, claiming it had been hacked.²¹ Scams like this cannot be tolerated. We can and must do more to block illegally spoofed calls before they ever reach consumers. The State AGs encourage the FCC to adopt rules authorizing providers to block these and other kinds of illegally spoofed calls.

D. STIR/SHAKEN Is Welcome Progress

Those concerned with battling illegal robocalls and illegal spoofing have been waiting for voice service providers to fully implement the STIR (Secure Telephone Intity Revisited) and SHAKEN (Secure Handling of Asserted information using toKENs)²² protocols – frameworks that service providers can utilize to authenticate legitimate calls and identify illegally spoofed calls. The State AGs see the industry is making progress concerning this initiative. On September 13, 2018, the Alliance for Telecommunications Industry Solutions ("ATIS")²³ filed a letter²⁴ at this docket announcing the launch of the Secure Telephone Identity Governance Authority ("STI-GA"), which is designed to ensure the integrity of the STIR/SHAKEN protocols. With the launch of the Governance Authority, the remaining protocols can be established. Reports indicate STIR/SHAKEN will be operational by some carriers throughout next year.²⁵

We strongly recommend the FCC explore ways to encourage all domestic and international service providers to aggressively implement STIR/SHAKEN. The capability to identify illegally

spoofed, scam calls will increase in proportion to the number of providers who adopt the STIR/SHAKEN protocols.²⁶ This is a positive step forward and we hope that as the implementation of STIR/SHAKEN continues to progress, the relevant participants, including the Governance Authority, will keep consumer organizations and the State AGs fully informed of their progress.

E. Conclusion – The Government and Industry Must Continue to Collaborate and Innovate

The pervasiveness of illegal robocalls and scam calls is a problem that cannot be solved by any one method, including the STIR/SHAKEN initiative. We, the undersigned State Attorneys General, need to continue to work together and in collaboration with our federal counterparts and the telecommunications industry to identify and implement new methods to combat the proliferation of these illegal acts. Also, we encourage the FCC to implement additional reforms, as necessary, to respond to technological advances that make illegal robocalls and illegal spoofing such a difficult problem to solve. Only by working together, and utilizing every tool at our disposal, can we hope to eradicate this noxious intrusion on consumers' lives.

BY THIRTY-FIVE (35) STATE ATTORNEYS GENERAL:



MARK BRNOVICH
Attorney General of Arizona



LESLIE RUTLEDGE
Attorney General of Arkansas



GEORGE JEPSEN
Attorney General of Connecticut



MATTHEW P. DENN
Attorney General of Delaware



KARL A. RACINE
Attorney General of the District of Columbia



PAM BONDI
Attorney General of Florida



STEPHEN H. LEVINS
Executive Director of Hawaii
Office of Consumer Protection



LISA MADIGAN
Attorney General of Illinois



CURTIS HILL
Attorney General of Indiana



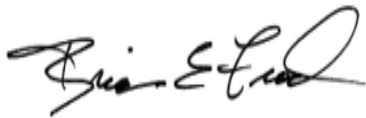
THOMAS J. MILLER
Attorney General of Iowa



DEREK SCHMIDT
Attorney General of Kansas



JEFF LANDRY
Attorney General of Louisiana



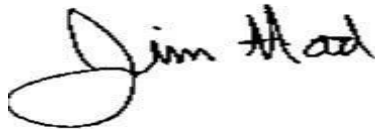
BRIAN E. FROSH
Attorney General of Maryland



MAURA HEALEY
Attorney General of Massachusetts



LORI SWANSON
Attorney General of Minnesota



JIM HOOD
Attorney General of Mississippi

TIM FOX
Attorney General of Montana

DOUGLAS J. PETERSON
Attorney General of Nebraska

ADAM PAUL LAXALT
Attorney General of Nevada

GORDON MACDONALD
Attorney General of New Hampshire

GURBIR S. GREWAL
Attorney General of New Jersey

HECTOR BALDERAS
Attorney General of New Mexico

BARBARA D. UNDERWOOD
Attorney General of New York

JOSH STEIN
Attorney General of North Carolina

WAYNE STENEHJEM
Attorney General of North Dakota

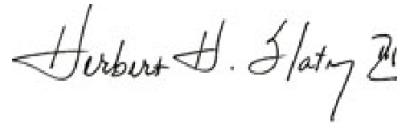
MIKE HUNTER
Attorney General of Oklahoma

ELLEN F. ROSENBLUM
Attorney General of Oregon

JOSH SHAPIRO
Attorney General of Pennsylvania



PETER F. KILMARTIN
Attorney General of Rhode Island



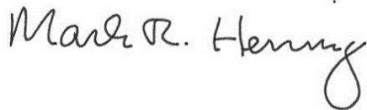
HERBERT H. SLATTERY III
Attorney General of Tennessee



SEAN D. REYES
Attorney General of Utah
Counsel for the State of Utah and
Utah Division of Consumer Protection



THOMAS J. DONOVAN, JR.
Attorney General of Vermont



MARK R. HERRING
Attorney General of Virginia



BOB FERGUSON
Attorney General of Washington



BRAD D. SCHIMEL
Attorney General of Wisconsin

DATE: OCTOBER 8, 2018

¹ Hawaii is represented in this matter by its Office of Consumer Protection, an agency which is not part of the state Attorney General’s Office, but which is statutorily authorized to undertake consumer protection functions, including legal representation of the State of Hawaii. For simplicity purposes, the entire group will be referred to as the “Attorneys General” or individually as “Attorney General” and the designations, as they pertain to Hawaii, refer to the Executive Director of the State of Hawaii’s Office of Consumer Protection.

² *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Public Notice, CG Docket No. 17-59, August 10, 2018, Bureau Seeks to Refresh the Record (“Public Notice”).

³ Caller ID spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. See <https://www.fcc.gov/consumers/guides/spoofing-and-caller-id>.

⁴ *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, CG Docket No. 17-59, November 17, 2017 (“2017 Call Blocking Order”) (FCC adopted rules allowing providers to block calls from phone numbers on a do-not-originate (“DNO”) list and calls from invalid, unallocated, or unused numbers).

⁵ Here we are referring to the patterns that emerge from the analyzing of call data, including but not limited to, call completion rates, average call durations, call volumes, times at which calls are placed, and sequential dialing patterns.

⁶ *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Comment of 30 State Attorneys General, CG Docket No. 17-59, filed July 6, 2017, pg. 1, 2, footnote 4 (number of consumer complaints from a sampling of States who signed on to the comment).

⁷ *See* <https://www.consumer.ftc.gov/articles/0381-how-does-robocall-work-infographic>.

⁸ *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Notice of Proposed Rulemaking and Notice of Inquiry, CG Docket No. 17-59, March 23, 2017, Statement of Chairman Ajit Pai. *See also* FTC Do Not Call Registry Data Book for Fiscal Year 2017 (over 4.5 million robocall complaints as opposed to approximately 2.5 million “live caller” complaints).

⁹ *See* <https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/national-do-not-call-registry-data-book-fy-2>. In 2014, the FTC received approximately 1.7 million illegal robocall complaints. In 2015, the number of complaints rose to over 2.1 million. In 2016, the number climbed to approximately 3.4 million complaints. Last year, the FTC received 4.5 million illegal robocall complaints.

¹⁰ *See* <https://www.cbsnews.com/news/how-to-stop-robocalls-those-annoying-automated-phone-calls-are-about-to-get-worse/>. *See also* <https://www.prnewswire.com/news-releases/robocall-epidemic-breaks-annual-record-with-305-billion-calls-in-2017-300580916.html>.

¹¹ *See* <https://www.prnewswire.com/news-releases/robocall-epidemic-breaks-annual-record-with-305-billion-calls-in-2017-300580916.html>.

¹² *Id.*

¹³ 16 C.F.R. § 310.4(b)(1)(v) (abusive telemarketing act or practice, and violation of *Telemarketing Sales Rule*, to initiate an outbound telephone call that delivers a prerecorded message).

¹⁴ *See* <https://www.cbsnews.com/news/how-to-stop-robocalls-those-annoying-automated-phone-calls-are-about-to-get-worse/>.

¹⁵ *See* <https://blog.truecaller.com/2017/04/19/truecaller-us-spam-report-2017/>.

¹⁶ Attorney General Shapiro shared a story of a Pennsylvania senior who fell victim to the “IRS scam.” In the scammer’s initial call to the senior, the caller ID displayed a number for the Pennsylvania State Police. The spoofing of government agency phone numbers to facilitate scams is all too common. *See for example* <https://www.fbi.gov/contact-us/field-offices/philadelphia/news/press-releases/phone-scam-uses-threats-spoofed-fbi-phone-numbers>.

¹⁷ 2017 Call Blocking Order, pg. 1, footnote 3 (Noting Attorney General Shapiro’s letter encouraging the FCC to move forward quickly to implement the rules).

¹⁸ *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Comment of 30 State Attorneys General, CG Docket No. 17-59, filed July 6, 2017.

¹⁹ <https://www.fcc.gov/consumers/guides/spoofing-and-caller-id>.

²⁰ In 2017, reports of caller ID spoofing, as well as neighbor spoofing have increased from previous years. *See Biennial Report to Congress*, Under the Do Not Call Registry Fee Extension Act of 2007, FTC, December 2017.

²¹ See <https://philadelphia.cbslocal.com/2018/04/11/scam-own-phone-number-calls/>.

²² See <https://transnexus.com/whitepapers/understanding-stir-shaken/>. See also Robocall Strike Force Report, October 26, 2016, pg. 5, (“The premise of STIR/SHAKEN is that telephone calls and the telephone numbers associated with the calls, when they are originated in a service provider network can be authoritatively and cryptographically signed by the authorized service provider, so that as the telephone call is received by the terminating service provider, the information can be verified and trusted. This set of industry standards is intended, as it is more fully deployed into the VoIP based telephone network, to provide a basis for verifying calls, classifying calls, and facilitating the ability to trust caller identity end to end. Illegitimate actors can then be more easily and quickly identified with the hope that telephone fraud is reduced significantly. While industry members believe that the SHAKEN framework holds considerable promise for repressing the presence of robocalling in the communications ecosystem, the Strike Force recognizes that the nature of bad actors and their tactics to harass consumers with unwanted robocalls and fraudulent, spoofed Caller IDs are ever changing and adapting. Further, carriers are at various stages of transitioning to IP-enabled networks and SHAKEN fundamentally depends upon IP network technologies.”)

²³ See <https://www.atis.org/> (“ATIS is a forum where the information and technology companies convene to find solutions to...shared challenges.”).

²⁴ See *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Letter, ATIS, September 13, 2018.

²⁵ See *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, *ex parte* filings, Verizon (5/7/18), Comcast (5/18/18), AT&T (5/16/18), and T-Mobile (5/24/18).

²⁶ See *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Comments of T-Mobile USA, Inc., September 24, 2018, pg. 4.