U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

April 30, 2019

TO: Republican Members, Subcommittee on Communications and Technology

FROM: Committee Republican Staff

RE: Hearing entitled "Legislating to Stop the Onslaught of Annoying Robocalls" Tuesday, April 30, 2019, at 10 a.m. in 2123 Rayburn HOB.

I. SUMMARY

- There is strong, bi-partisan support for a legal framework that targets illegal robocalls from bad actors who intend to scam and defraud Americans.
- Any framework must continue to allow pro-consumer calls that consumers want, such as prescription refill reminders or credit card monitoring, without over-burdening the legitimate callers.
- Legislative efforts should focus on preventing the bad actors before tackling issues related to legitimate callers.

II. WITNESSES

- **Patrick Halley**, Senior Vice President, Advocacy and Regulatory Affairs, USTelecom – The Broadband Association;
- **Aaron Foss**, Founder, Nomorobo;
- **Dave Summitt**, Chief Information Security Officer, H. Lee Moffitt Cancer Center & Research Institute, Fellow for the Institute for Critical Infrastructure Technology; and,
- **Margot Saunders**, Senior Counsel, National Consumer Law Center.

III. BACKGROUND

Unwanted and illegal robocalls comprise the largest complaint category received by both the Federal Communications Commission (FCC) and Federal Trade Commission (FTC). In just one year, US consumers received an estimated 2.4 billion robocalls per month.[1] These robocalls come from bad actors who use autodialing technology to scam consumers, often by maliciously "spoofing" their caller ID information to mask the caller's true identity and instead make the call

[1] https://www.fcc.gov/about-fcc/fcc-initiatives/fccs-push-combat-robocalls-spoofing

appear like it is coming from a local source. Hard-working Americans have been tricked into picking up countless calls like this and then have been bullied into paying what they think is an outstanding debt, only to send money or some other form of compensation to the fraudster who maliciously spoofed the phone number with the intent to deceive and scam.[2]

Separate from the unwanted and illegal robocalls made by scammers and fraudsters, legitimate parties also harness autodialing technology to provide important alerts for a variety of needs that consumers want. For example, many school districts use autodialing technology to notify parents if there is a change in school status, such as a snow day; doctors' offices and hospitals use autodialing technology to remind patients of surgical after-care instructions or prescription refill information; and public safety officials use autodialing technology to alert communities of wildfires and evacuation notices.

The FCC, with support from Congress, has focused on combatting unlawful robocalls and malicious caller ID spoofing. Last year's RAY BAUM's Act prohibited spoofing calls or texts originating outside the United States, and tasked the FCC with conducting a rulemaking on the subject.[3] Congress, as part of RAY BAUM's Act, also required the FCC to work with the FTC to educate consumers on identifying spoofed calls, and directed the Government Accountability Office to conduct a study on fraudulent, misleading, or inaccurate caller ID information.

The FCC has also proposed and implemented a variety of policy initiatives to combat unwanted, illegal calls. In November 2017, the FCC adopted rules to allow telecommunications carriers to block calls from numbers that cannot make outgoing calls.[4] In December 2018, the FCC adopted rules that would reduce unwanted calls to reassigned numbers through the creation of a database.[5] Furthering this policy work, the FCC has imposed major fines on malicious caller ID spoofers.[6]

Industry has also aided these efforts by providing solutions to the problem by developing a set of procedures to authenticate caller ID information associated with telephone calls and assign these calls a secure, encrypted certificate. These technical standards are referred to as STIR-SHAKEN, which is an acronym for Signature-based Handling of Asserted Information Using toKENs (SHAKEN) and the Secure Telephone Identity Revisited (STIR) standards. The FCC accepted these recommendations, and industry is moving quickly to establish this industry-developed call authentication system.[7] The FCC has called on industry providers to adopt and implement this call authentication system by November 2019 in order to combat illegal caller ID spoofing.[8]

---

[2] https://www.irs.gov/newsroom/irs-urges-public-to-stay-alert-for-scam-phone-calls
[3] Public Law 115-141, Division P, Section 503.
[4] https://www.fcc.gov/document/fcc-adopts-rules-help-block-illegal-robocalls
[5] https://www.fcc.gov/document/fcc-creates-reassigned-numbers-database-combat-unwanted-robocalls-0
[6] https://docs.fcc.gov/public/attachments/FCC-18-58A1.pdf; https://docs.fcc.gov/public/attachments/FCC-18-134A1.pdf; https://docs.fcc.gov/public/attachments/FCC-18-135A1.pdf
[7] https://docs.fcc.gov/public/attachments/DOC-350690A1.docx
[8] https://www.fcc.gov/document/chairman-pai-demands-industry-adopt-protocols-end-illegal-spoofing

Outside of the call authentication framework, industry has offered other tools to protect consumers from illegal, unwanted robocalls. Some carriers have implemented solutions that allow consumers to protect themselves from scams by notifying the consumer that the call is likely from a scammer or blocking all likely scammers before the call even reaches the consumer.[9] In addition to the carrier-based solutions, there are a variety of other app-based solutions already in effect.[10]

IV. DISCUSSION

Despite the tremendous progress that has been made to curb illegal and fraudulent robocalls, work remains. Congress, the FCC, the FTC, and industry must continue to deter these unwanted and illegal robocalls. Several legislative proposals would help close some of the current-loopholes to provide information when the agencies seek out these fraudsters. There are also tools that industry can automatically provide to consumers to help deter some of the calls that are highly likely to be maliciously spoofed with the intent to defraud. By focusing on the illegal, and unwanted robocalls from bad actors with the intent to scam and defraud, Americans will once again trust their phones and be able to continue receiving the life-saving information and useful calls and texts that they want.

V. STAFF CONTACTS

Please contact Robin Colwell or Tim Kurth of the Republican Committee staff at (202) 225-3641 if you have questions about the hearing.

[9] https://www.t-mobile.com/resources/call-protection
[10] https://www.pcmag.com/feature/362120/how-to-block-robocalls-and-spam-calls