Written Testimony of Patrick Halley
Senior Vice President, Advocacy and Regulatory Affairs
USTelecom – The Broadband Association

"Legislating to Stop the Onslaught of Annoying Robocalls"

April 30, 2019

Chairman Doyle, Ranking Member Latta, Members of the Subcommittee, thank you for giving me the opportunity to appear before you today. My name is Patrick Halley, and I am Senior Vice President of Advocacy and Regulatory Affairs at USTelecom – The Broadband Association.

USTelecom is the nation's trade association representing broadband providers, suppliers, and innovators connecting our families, communities and enterprises to the future. Our diverse membership ranges from large publicly traded global communications providers, manufacturers, and technology enterprises, to small companies and cooperatives – all providing advanced communications services in urban and rural markets, and everything in between.

USTelecom and our members share this Subcommittee's desire to eliminate the plague of illegal and unwanted robocalls and we appreciate your focus on potential solutions to address the problem. Along with our members, we are working daily to enhance our knowledge about the calls that traverse our networks in order to block illegal calls and provide consumers with more information about the calls they receive. Our efforts are designed to empower consumers by providing more information about the identity of callers and enabling them to block calls they do not wish to receive. We do this because our customers demand it, because it undoubtedly reduces the ability of fraudsters to achieve their objectives, and because it increases the confidence of consumers and businesses that rely on our networks. As the FCC recently stated, "it is obvious that the volume of unwanted calls is reducing the value of telephony to anyone who makes or receives calls."[1] This is a problem the industry is committed to solving.

In addition to improving the consumer experience, we are equally focused on facilitating enhanced coordination with federal and state enforcement authorities, including the Federal Communications Commission (FCC), the Federal Trade Commission (FTC) and state Attorneys General. By helping law enforcement agencies quickly identify the source of illegal callers, together we can bring criminals to justice. The ongoing civil enforcement efforts of the FCC and the FTC are critical. However, increased criminal enforcement against illegal robocallers is necessary.

As the Subcommittee considers potential legislative actions to address the robocall plague, I would like to highlight three areas of active industry leadership to address the problem.

[1] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Second Report and Order, FCC 18-177, CG Docket No. 17-59 at para. 4 (Dec. 2018) (describing the "multi-prong approach" to address the problem of unwanted calls).

- First, industry has undertaken considerable efforts to deploy call authentication technologies, commonly referred to as STIR/SHAKEN, that will substantially diminish the ability of illegal robocallers to spoof caller-ID information. Companies of all types and sizes are deploying these standards into their IP networks today and will continue to do so throughout 2019. Once deployed, consumers will have more information about the identity of a caller or the type of call they are receiving. And carriers will be able to more accurately identify the source of calls, which will improve call traceback efforts.

- Second, more tools are available today than ever before for consumers to mitigate illegal or unwanted robocalls. A significant number of voice providers are increasingly integrating these tools into their networks and hundreds of applications are available to consumers on their smartphones.

- Third, USTelecom's Industry Traceback Group ("Traceback Group") is expanding its efforts to identify the source of illegal robocalls and working in close coordination with federal and state agencies to assist in enforcement efforts. Recently, we have significantly enhanced our ability to traceback calls by automating the process. The time it now takes to trace back illegal robocalls has been reduced from weeks to days – sometimes even hours.

Beyond simply implementing STIR/SHAKEN and participating in the Traceback Group, many carriers are taking steps to require others to do the same. Our members do not want to do business with other carriers that are not taking sufficient steps to address the problem. For example, some carriers are amending their contracts so that the entire call path for calls received from upstream carriers is with companies that are participating in traceback efforts. In addition, carriers are actively monitoring traffic over their networks to ensure their customers are not making illegal calls, and to identify other providers that appear to be carrying illegal traffic – and then taking steps to help those other carriers fix the problem or to no longer do business with them.

As the FCC's Chief Technology Officer and Enforcement Bureau Chief noted in recent letters to providers encouraging participation in the USTelecom Industry Traceback Group, "neither government, nor industry, without the active assistance of the other, can hope to stem the flood of scam calls plaguing consumers across the country."[2] USTelecom greatly appreciates the collaborative work we do with our partners in government and we welcome the opportunity to work with Congress on additional steps that can be taken.

Industry is Committed to the Deployment of Call Authentication Standards.

Industry is swiftly moving to implement the STIR/SHAKEN call authentication standard. Once implemented, the ability of illegal robocallers to spoof caller-ID information will be significantly reduced and consumer knowledge about the validity of incoming calls will substantially increase. Last year, the industry-led Governance Authority for the SHAKEN standard was established under The Alliance for Telecommunications Industry Solutions (ATIS), the standards body coordinating industry implementation of the SHAKEN protocol. And next

[2] Press Release, FCC, FCC Calls on Network Voice Providers to Join Effort to Combat Illegal Spoofed Scam Robocalls (Nov. 6, 2018), https://docs.fcc.gov/public/attachments/DOC-354942A1.pdf.

month, ATIS is expected to identify the Policy Administrator that will oversee the day-to-day operations of the SHAKEN standard.

Numerous voice providers – representing the wireline, wireless, and cable industries – have committed to deploying the SHAKEN and STIR standards within their respective networks.[3] While deployment depends on the timely and practical availability of vendor network upgrades and applications and there are some differences in the specific timelines to deployment of the SHAKEN and STIR standards, implementation efforts started in 2018, with most targeting deployments in their IP networks as soon as the end of 2019. Testing of the new technology and products is well under way. In March, AT&T and Comcast successfully verified authentication of calls between their separate networks, and Verizon announced the first exchange of STIR/SHAKEN-enabled calls to and from wireless customers.

While deployment of the SHAKEN and STIR standards is not a panacea to the robocall problem, these standards will improve the reliability of the nation's communications system by better identifying legitimate traffic. The deployment of the SHAKEN standard will also facilitate the ability of stakeholders (such as USTelecom's Traceback Group) to identify illegal robocalls and the sources of untrustworthy communications.

Robocall Mitigation Tools are Increasingly Available to Consumers Across a Variety of Voice Platforms.

Voice providers themselves and independent application developers are increasingly offering services that can help Americans reduce unknown and potentially fraudulent calls. Like efforts to authenticate calls, these tools alone will not solve the robocall problem, but they are an important tool that empowers consumers with the ability to better identify and/or block illegal or unwanted robocalls.

Importantly, facilities-based providers are increasingly developing robocall mitigation tools themselves, including within their networks. For example, AT&T's "Call Protect" service for customers with IP wireline phones, iPhones and HD Voice enabled Android handsets automatically blocks suspected fraudulent calls.[4] When activated, AT&T will automatically block fraudulent calls, warn of suspected spam calls, and allow consumers to block unwanted calls from a specific number.

In addition, through its Spam Alerts service, for all wireline customers who have Caller ID (including ones served on legacy copper technology), Verizon provides enhanced warnings about calls that meet Verizon's spam criteria by showing the term "SPAM?" before a caller's name on the Caller ID display. Using TNS's Call Guardian and Neustar's Robocall Mitigation solution, the Spam Alerts feature proactively identifies and warns customers about potentially malicious robocalls. Verizon has also rolled out free spam alerting and call blocking tools to wireless customers whose smartphones support these features. Consumers can better decide if they want to answer a particular call, or they can choose to have spam calls sent straight to

[3] *See e.g.*, FCC, Combating Spoofed Robocalls with Caller ID Authentication, https://www.fcc.gov/call-authentication (last visited Apr. 28, 2019).
[4] *See* AT&T, AT&T Mobile Security & Call Protect, https://www.att.com/features/security-apps.html (last visited Apr. 28, 2019).

voicemail.

Carriers, including USTelecom members CenturyLink, Windstream, Frontier, Consolidated and others, are also deploying a variety of additional tools across their TDM and IP networks, including "anonymous call rejection" services that block callers who intentionally mask their phone numbers and "no solicitation" services that make unidentified callers go through a screening step before ringing. Multiple service providers also work with Nomorobo to facilitate their customers' ability to use that third-party blocking service. Additionally, Metaswitch provides a robocall blocking service that supports all voice infrastructure and switches, from legacy Class 5 TDM to Metaswitch's pure VoIP systems.[5]

There are also numerous third-party scoring and labelling analytics tools for wireless consumers. In 2016, there were approximately 85 call-blocking applications available across all platforms. By October 2018, there were over 550 applications available, a 495% increase in call blocking, labeling, and identifying applications to fight malicious robocalls. The multitude and diversity of tools across multiple platforms is a testament to industry's commitment to empower consumers, regardless of the type of network involved.

Industry Traceback Efforts are Critical to Identifying the Source of Illegal Robocalls.

Equally important for reducing illegal robocalls is the ability to identify the source of calls and a strong partnership between industry and government to share such information to go after bad actors. USTelecom leads the Industry Traceback Group whose members are committed to identifying the source of illegal robocalls, and working with law enforcement to bring these illegal actors to justice. The FCC's 2017 Strike Force Report contains a detailed overview of the Traceback Group.[6]

There are currently 27 members of the Traceback Group, including traditional wireline phone companies, wholesale carriers, wireless providers, and cable companies. The membership also includes foreign carriers (*e.g.*, Bell Canada), and non-traditional voice providers (*e.g.*, Google and YMax).[7] The Communications Act permits voice providers to share customer proprietary network information (CPNI) in order to protect their customers and/or networks, enabling USTelecom's Traceback Group to quickly and efficiently identify the path of calls under investigation.[8]

Since late 2017, USTelecom has been making enforcement referrals to the FCC and the FTC based on the traceback results of the group. This industry/government partnership helps to

---

[5] *See* Metaswitch, Robocall Blocking Service, https://www.metaswitch.com/solutions/fixed-line-solutions/robocall-blocking-service) (last visited April 28, 2019).

[6] *See* Letter from Brian Scarpelli, Senior Policy Counsel, ACT – The App Association; Thomas E. Goode, General Counsel, ATIS; Krista Witanowski, Ass't Vice President, Regulatory Affairs, CTIA; and Kevin G. Rupy, Vice President, Law & Policy, USTelecom, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59 at 19 – 23 (filed Apr. 28, 2017), available at: https://ecfsapi.fcc.gov/file/10428413802365/Ex%20Parte-Strike-Force-Report-2017-04-28-FINAL.pdf.

[7] *See* Appendix for list of Industry Traceback Group participating companies.

[8] Section 222(d)(2) of the Communications Act permits telecommunications carriers to share, disclose and/or permit access to, CPNI in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." 47 U.S.C. § 222(d)(2).

streamline the enforcement efforts of both the FCC and the FTC who can now avoid the time-consuming process of issuing subpoenas to every provider in the call path. Instead, they can more efficiently focus their efforts only on those upstream providers that have declined to cooperate with the efforts of the Traceback Group. Late last year, the FCC acknowledged that USTelecom's manual traceback process had reduced the time necessary for the agency to conduct its own traceback investigations from "months to weeks" and called the Traceback Group's work "instrumental" in helping the Commission to achieve its goal of taking swift action against illegal robocallers.[9] Recently, USTelecom modified its previous manual traceback process to one that is largely automated. The automated process will enable a significantly greater number of tracebacks and dramatically reduces the amount of time for each traceback. These efficiencies will better assist investigations by the FCC and the FTC.

While numerous providers have joined USTelecom's Traceback Group, and many others cooperate in good faith, several upstream carriers refuse to cooperate. This not only prevents the Traceback Group from identifying the true origin of some calls, but it makes subsequent law enforcement investigations more time consuming. Given the crucial role of traceback in mitigating illegal robocalls, Congress and federal enforcement agencies should strongly encourage voice providers to participate in traceback efforts. To that end, while we are still assessing its potential impact, we appreciate the objectives of Rep. Latta's discussion draft "STOP Robocalls Act" that, in part, seeks to ensure call information from interconnected VoIP, including one-way VoIP services, is available for tracebacks.

More Criminal Enforcement of Illegal Robocallers is Necessary.

Ongoing federal civil enforcement efforts are essential. For example, the FCC last year approved a $120 million fine against one illegal robocaller responsible for generating billions of calls. The FTC recently issue fines ranging from $500,000 to $3.6 million and shut down four separate operations responsible for bombarding consumers nationwide with billions of unwanted and illegal robocalls pitching auto warranties, debt-relief services, home security systems, fake charities, and Google search results.[10]

These civil enforcement efforts are critical, and we support the objectives of Chairman Pallone's "Stopping Bad Robocalls Act" to allow the FCC to go after first time offenders and to increase the statute of limitations for such enforcement efforts. However, there is an acute need for aggressive criminal enforcement against illegal robocallers at the federal and state level. Criminal organizations and individuals engaged in illegal robocalling activity should be identified, targeted and brought to justice through criminal enforcement efforts. We applaud the proposed legislation by members of this subcommittee seeking to increase forfeiture penalties. However, fines alone are insufficient. Of particular note in the FTC's recent announcement is the acknowledgement that two of the individuals named in the complaint are "recidivist robocallers," who were each targeted in earlier FTC lawsuits brought in 2017 and 2018. Beyond

[9] *See* Letter from Rosemary Harold, Chief, Enforcement Bureau, FCC, and Eric Burger, Chief Technology Officer, FCC, to Jonathan Spalter, President and CEO, USTelecom at 1 (Nov. 6, 2018), available at: https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf.

[10] *See* Press Release, FTC, FTC Crackdown Stops Operations Responsible for Billions of Illegal Robocalls, (rel. March 26, 2019) https://www.ftc.gov/news-events/press-releases/2019/03/ftc-crackdown-stops-operations-responsible-billions-illegal.

these civil penalties, those who blatantly disobey the law and who enable fraudulent activity need to go to jail. USTelecom and its industry partners stand ready to assist the government in bringing these bad actors to justice. Indeed, the ultimate goal of USTelecom's Traceback Group is to identify the source of the worst of these illegal calls, and enable further enforcement actions by federal agencies.

U.S. Attorneys' offices across the country should prioritize enforcement where federal statutes, such as the Truth in Caller ID Act, are implicated, and should work closely with the FCC and FTC and international partners in enforcement cases, particularly when the calls originate outside of the United States. Another possible vehicle could be the Task Force on Market Integrity and Consumer Fraud, comprised of a number of divisions of the Department of Justice (DOJ), including the FBI and various United States Attorney's Offices as designated by the Attorney General.[11] The focus of the Task Force is to investigate and prosecute consumer and corporate fraud that targets the public and the government, with a particular emphasis on the elderly, service members and veterans. Given its focus on fraud directed towards consumers, as well as the inclusion of criminal enforcement agencies, the Task Force could be an ideal vehicle for pursuing criminal enforcement against illegal robocallers. The Spam Calls Task Force Act of 2019's proposed establishment of an interagency working group under the Attorney General, would also further enhance federal and state criminal law enforcement efforts against illegal robocallers.

There is no single solution to ending the scourge of robocalls, but progress is being made every day. USTelecom and our members – along with our wireless and cable partners – are strongly committed to working together with government to substantially reduce, and ultimately eliminate this problem.

[11] *See* Exec. Order No. 13844, 83 Fed. Reg. 33115 (July 11, 2018) available at: https://www.whitehouse.gov/presidential-actions/executive-order-regarding-establishment-task-force-market-integrity-consumer-fraud/.

Appendix: USTelecom Industry Traceback Participants

- Alliance
- ANI Networks
- AT&T
- Bandwidth
- Bell Canada
- Brightlink
- CenturyLink
- Charter
- Cincinnati Bell
- Comcast
- Consolidated
- Cox
- Frontier
- Google
- IDT Telecom
- Impact Telecom
- Inteliquent
- NovaTel
- O1 Communications
- Peeress
- Silver Star
- Sprint
- T-Mobile
- Verizon
- West Telecom
- Windstream
- YMax