Written Testimony of Kevin Rupy
On Behalf of USTelecom – the Broadband Association

"Illegal Robocalls: Calling All To Stop The Scourge"
April 11, 2019

Chairman Thune, Ranking Member Schatz, Members of the Subcommittee, thank you for giving me the opportunity to appear before you today.

My name is Kevin Rupy, and I am a Partner in the Telecommunications, Media, and Technology Practice at Wiley Rein LLP, and I am here today on behalf of USTelecom – The Broadband Association. USTelecom shares the Committee's concerns on illegal robocalls, and is pleased to support the TRACED Act.

Since I last testified before the Senate in 2018, there have been three substantial developments in the area of illegal robocalls, and I will also emphasize a fourth point.

- First, since last year, industry has undertaken considerable efforts to deploy call authentication technologies, commonly referred to as SHAKEN/STIR, that will substantially diminish the ability of illegal robocallers to spoof caller-ID information. Companies are deploying these standards into their IP networks today and will continue to do so throughout 2019.

- Second, consumers today have more tools than ever at their disposal to mitigate illegal or unwanted robocalls. Hundreds of such tools are available to consumers on their smartphones and a broad range of voice providers are increasingly integrating these tools into their networks.

- Third, USTelecom's Industry Traceback Group ("ITB Group") efforts, which seek to identify illegal robocallers, have been significantly enhanced through recent automation of the traceback process. The time it now takes to trace back illegal robocalls has been reduced from weeks to days – sometimes even hours.

- Fourth, while the federal civil enforcement actions of the Federal Communications Commission (FCC) and Federal Trade Commission (FTC) are laudatory and effective, increased criminal enforcement against illegal robocallers is needed.

Industry Has Demonstrated a Strong Commitment to the Deployment of SHAKEN/STIR.

First, the industry-led Governance Authority for the SHAKEN standard was established last year under The Alliance for Telecommunications Industry Solutions (ATIS), the standards body coordinating industry implementation of the SHAKEN protocol. ATIS will identify the Policy Administrator in May, that will oversee the day-to-day operations of the SHAKEN standard. In short, industry is swiftly moving to implement this important call authentication technology. Once implemented, the ability of illegal robocallers to spoof caller-ID information will be significantly reduced, while consumer knowledge about the validity of incoming calls will increase.

Central to this effort is the development of the separate SHAKEN and STIR standards and best practice implementations. While deployment of the SHAKEN and STIR standards is not a panacea to the robocall problem, these standards should 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 ITB Group) to identify illegal robocalls and the sources of untrustworthy communications.

There is strong industry commitment to the deployment of the SHAKEN and STIR standards. Numerous voice providers – representing the wireless, wireline and cable industries – have committed to deploying the SHAKEN and STIR standards within their respective networks. These include commitments from several companies with nationwide wireless coverage, as well as several large facilities based voice providers.[1] While there are some differences in the specific timelines to deployment of the SHAKEN and STIR standards, and deployment depends on the timely and practical availability of vendor network upgrades and applications, the commitments generally reflect deployments starting in 2018, with most targeting deployments in their IP networks as soon as the end of 2019.

In addition, the Call Authentication Trust Anchor Working Group (CATA WG) of the North American Numbering Council (NANC) completed its work last year to investigate a variety of issues associated with the SHAKEN/STIR system.[2] Testing of the new technology and products is well advanced. Just last month, Comcast and AT&T 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.

After issuing its report to the FCC, the NANC CATA WG also selected a Governance Authority to establish the policies for the SHAKEN certificate management framework. The Governance Authority – ATIS – has moved forward with its work. The Board of Directors for the Governance Authority was selected last year, and includes representatives from a broad range of industry constituencies, including large and small voice providers, as well as a diversity of network providers. The diversity and commitment of the Governance Authority Board of Directors will help to facilitate a controlled and productive deployment of the SHAKEN standard.

An Increasing Number of Robocall Mitigation Tools are Available to Consumers Across Multiple Voice Platforms, Including TDM.

Today, a broad range of voice providers, independent application developers and a growing number of diverse companies are offering services that can help Americans reduce unknown and potentially fraudulent calls. While these tools are not a panacea to the robocall problem, they are

---

[1] *See e.g.*, FCC website, *Combating Spoofed Robocalls with Caller ID Authentication*, (available at: https://www.fcc.gov/call-authentication) (visited April 9, 2019).

[2] See, Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR NANC Call Authentication Trust Anchor Working Group (available at: http://nanc-chair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf) (visited April 8, 2019).

an important component that empowers consumers with the increased ability to better identify and/or block illegal or unwanted robocalls. Of particular note, an increasing number of robocall mitigation tools are being deployed by facilities-based providers themselves.

For example, AT&T has launched its 'Call Protect' service that allows customers with iPhones and HD Voice enabled Android handsets to automatically block suspected fraudulent calls. AT&T also offers AT&T Digital Call Protect for IP wireline phones.[3] When the app is installed and set up, AT&T will automatically block fraudulent calls, warn of suspected spam calls, and allow consumers to block unwanted calls from a specific number for free.

In addition, last year, Verizon launched its Spam Alerts service which provides its wireline customers who have Caller ID – whether they are on copper or fiber – with 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. Verizon's Spam Alerts feature utilizes TNS's Call Guardian and Neustar's Robocall Mitigation solution to proactively identify illegal robocalls and other fraudulent caller activity with more accuracy. By using existing Caller-ID technology, the service empowers consumers to better decide if they should answer a particular call. Verizon has also rolled out spam alerting and call blocking tools to wireless customers whose smartphones support these features.

Carriers 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. Numerous service providers have worked with or are currently working with Nomorobo to facilitate their customers' ability to use that third-party blocking service, such as Verizon's "one click" solution that simplifies customers' ability to sign up for the service. In addition, the company Metaswitch also provides a robocall blocking service that supports all voice infrastructures and switches, from legacy Class 5 TDM to Metaswitch's pure VoIP systems.[4]

In the wireless arena, the number of scoring and labelling analytics tools for consumers has exploded. In 2016 there were approximately 85 call-blocking applications available across all platforms, including several offered by carriers to their customers at no charge. By October, 2018, there were over 550 applications available, a 495% increase in call blocking, labeling, and identifying applications to fight malicious robocalls. The diversity in tools across multiple platforms demonstrates industry's commitment to empower consumers, regardless of the type of network utilized by their chosen voice service provider.

---

[3] See, AT&T website, AT&T Mobile Security & Call Protect (available at: https://www.att.com/features/security-apps.html) (visited April 8, 2019).

[4] See, Metaswitch website, Robocall Blocking Service, (available at: https://www.metaswitch.com/solutions/fixed-line-solutions/robocall-blocking-service) (visited April 8, 2019).

Industry Traceback Efforts are Crucial to Combatting the Scourge of Illegal Robocalls.

An equally important tool for reducing illegal robocalls is a robust traceback process with vigorous and consistent enforcement action. Since 2016, USTelecom has led the 26-member ITB Group whose members are committed to identifying the source of illegal robocalls, and working with law enforcement to bring these illegal perpetrators to justice. The 2017 Strike Force Report contains a detailed overview of the Traceback Group, and its general structure and operations.[5]

There are currently twenty-six members of the ITB Group, which includes 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).

Since late 2017, USTelecom has been making enforcement referrals to the FCC and the FTC. This cooperation between industry and government can help to administratively streamline the enforcement efforts of both the FCC and the FTC. 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 ITB Group to quickly and efficiently identify the path of calls under investigation.[6]

This in turn, means that neither the FCC nor the FTC must go through the time-consuming process of issuing subpoenas to each and every provider in the call path – instead, they can focus such efforts only on those upstream providers that have declined to cooperate with the efforts of the Traceback Group. Indeed, just 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."[7]

The most significant development regarding USTelecom's ITB Group is the last year's transition of USTelecom's its manual traceback process to one that is largely automated. The automated process is expected to produce even greater efficiencies for both ITB Group tracebacks, as well

---

[5] *See*, Ex Parte Notice, from USTelecom, CTIA, ATIS, and ACT – The App Association, CG Docket No. 17-59, pp. 19 – 23 (submitted April 28, 2017) (available at: https://ecfsapi.fcc.gov/file/10428413802365/Ex%20Parte-Strike-Force-Report-2017-04-28-FINAL.pdf) (visited Sept. 24, 2018).

[6] Section 222(d)(2) of the Communications Act permits telecommunications carriers to share, disclose and/or permit access to, Customer Proprietary Network Information 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." See, 47 U.S.C. § 222(d)(2).

[7] *See*, Letter from Rosemary Harold, Chief, Enforcement Bureau, and Eric Burger, Chief Technology Office, to Jonathan Spalter, President and CEO, USTelecom, p. 1, November 6, 2018 (available at: https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf) (visited April 8, 2019).

as subsequent investigations by the FCC and the FTC.

While numerous providers have joined USTelecom's ITB Group, and many others cooperate in good faith, too many upstream carriers refuse to cooperate. This not only prevents the ITB Group from identifying the true origin of these malicious calling events, 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.

Criminal Enforcement of Illegal Robocallers is Needed.

Finally, while current federal enforcement efforts are laudatory, they are mostly limited to civil enforcement. There is an acute need for aggressive criminal enforcement against illegal robocallers at federal and state levels. Criminal syndicates engaged in illegal robocalling activity should be identified, targeted and brought to justice through criminal enforcement efforts. We applaud the TRACED Act's facilitation of these criminal enforcement efforts.

USTelecom applauds government efforts in the robocall fight, particularly the ongoing civil enforcement actions by the FCC and FTC. For example, the FCC last year, approved a $120 million fine against one illegal robocallers responsible for generating billions of calls. The FTC also continues to engage in a series of complementary enforcement actions that target the worst of the worst bad actors in this space.

These civil enforcement actions brought by both agencies send a strong and powerful message to illegal robocallers that they will be located and brought to justice. USTelecom and its industry partners stand ready to further assist in these efforts to bring these bad actors to justice. Indeed, the ultimate goal of USTelecom's ITB Group is to identify the source of the worst of these illegal calls, and further enable further enforcement actions by federal agencies.

While current federal enforcement efforts are laudatory, they are mostly limited to civil enforcement. As a result, bad actors currently engaged in criminal robocall activities are – at most – subject only to civil forfeitures. USTelecom believes there is an acute need for coordinated, targeted and aggressive criminal enforcement of illegal robocallers at the federal level and in conjunction with state attorneys general. Given the felonious nature of their activities, criminal syndicates engaged in illegal robocalling activity should be identified, targeted and brought to justice through criminal enforcement efforts.

To further underscore the need for criminal enforcement of illegal robocallers, the FTC announced this month that it reached a settlement with four separate operations, two of which allegedly facilitated "billions of illegal robocalls to consumers nationwide."[8] Of particular note in the FTC's announcement is the acknowledgement that two of the individuals named in the complaint are "recidivist robocallers," who were each targeted in FTC lawsuits brought in 2017

[8] *See*, FTC Press Release, *FTC Crackdown Stops Operations Responsible for Billions of Illegal Robocalls*, March 26, 2019 (available at: https://www.ftc.gov/news-events/press-releases/2019/03/ftc-crackdown-stops-operations-responsible-billions-illegal) (visited April 8, 2019).

and 2018. In fact, the FTC noted that certain of these recidivist robocallers were "permanently banned from making robocalls, or assisting others in doing so."[9]

It is clear that more than civil enforcement is necessary to address illegal robocalling. We believe, in particular, that 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.[10] 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 TRACED Act's establishment of an interagency working group under the Attorney General, will also further enhance federal and state criminal law enforcement efforts against illegal robocallers.

While a holistic approach is essential to broadly address the issue of robocalls, robust enforcement efforts targeting illegal robocallers are most effective since they address the activity at the source. For example, consumer-centric tools may stop a series of calls from reaching tens of thousands consumers, whereas root-cause removal stops millions of calls from ever being dialed.

[9] *Id.*

[10] See, White House Executive Order, Executive Order Regarding the Establishment of the Task Force on Market Integrity and Consumer Fraud, July 11, 2018 (available at: https://www.whitehouse.gov/presidential-actions/executive-order-regarding-establishment-task-force-market-integrity-consumer-fraud/) (visited July 20, 2018).