Timothy P. McKone
Executive Vice President
Federal Relations

AT&T Services, Inc.
1120 20th Street, NW
Suite 800
Washington, DC 20036

T 202.463.4144
tm3703@att.com
att.com

October 13, 2017

Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

I am responding to your September 14, 2017, letter to Randall Stephenson, AT&T Chairman and CEO, regarding the Signaling System 7 ("SS7") network.

Like you, we take any threat to our network and our customers' communications seriously. We have been actively assessing and responding to known SS7 threats for some time, and just as these threats can evolve over time, so do our means to identify and mitigate them.

As you know, SS7 is a signaling protocol that allows carriers to communicate with each other to deliver calls and text messages between their networks. Over the last half-century, SS7 has been integral to the explosion of telecommunications competition and advanced technology. Among other things, SS7 makes it possible for wireless customers to roam globally, spurring the rapid growth of wireless technology around the world. It also supports enhanced features, such as call forwarding and caller ID, all to the benefit of consumers.

This expanded use of SS7 offers great benefits, but also presents evolving risk. Unlike cybersecurity threats from hackers, the growing number of carriers having *legitimate* credentials into the network creates the threat to SS7. At its inception, in the 1970s, roughly 10 trusted carriers worldwide had access to the SS7 network. With the explosion of competition, international calling and roaming, hundreds of carriers now have access to SS7, many of them in unstable or unfriendly nations where credentials can be compromised – and, as you note, even sold on the open market for a fee. AT&T has therefore hardened and tuned our defenses to account for these developments given that the trust model is no longer fully reliable.

Moreover, given the importance of the SS7 system to global communications and interconnection between networks, any carrier response to a SS7 vulnerability must be mindful of the legitimate uses of SS7. Prior to implementation of any defense, a carrier must carefully research how its actions might impact its network. AT&T alone handles tens of billions of SS7 messages per day. And the clear majority of SS7 messages are legitimate, enabling consumers to complete critical communications. As the FCC SS7 working group concluded: "because the overwhelming amount of SS7 traffic is legitimate, carriers need to be measured as they implement solutions to avoid collateral network impacts."[1]

[1] FCC CSRIC Working Group 10 Final Report: Legacy Systems Risk Reductions (March 2017), at 11. https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf

Against this backdrop, AT&T has employed an aggressive, multifaceted approach to the SS7 threat. We would be glad to provide you more specific information concerning our strategy in an appropriate, confidential setting, as we have already done with your staff. However, public disclosure of the specific technology we have deployed to meet any cybersecurity threat (and where we stand in implementing those defenses) would only provide bad actors a blueprint for how to evolve their techniques and defeat our defenses. We trust that you appreciate that, to best protect our network and our customers, we must closely guard this information.

Nonetheless, we can confirm that AT&T has taken significant, aggressive steps to protect the SS7 network. For example:

- We have implemented extensive blocking and filtering of nefarious SS7 messages, including blocking of the vulnerabilities identified by researchers, industry groups and our own testing. We have also implemented "SMS Home Routing."

- We have, alone and in concert with our vendors, implemented new firewalls and other innovative technologies to monitor, inspect and filter nefarious traffic.

- We are in the final stages of implementing the GSM Association (GSMA) best practices on protecting SS7, with most of the work behind us.

- We have tested our network and worked with outside experts to better understand and assess the threat to SS7, as we routinely do with network security threats. We have responded to issues identified in such testing and will continue to do so as threats evolve. Our testing has shown that our aggressive steps to meet the threat are working.

- We have collaborated with the Department of Homeland Security (DHS), the intelligence community, and the industry to share information concerning potential threats and our responses.

This last point above concerning our work with DHS merits emphasis. Among other things, we participated with DHS on the FCC's nine-month-long working group in its Communications Security, Reliability and Interoperability Council (CSRIC) to study the SS7 risk and provide recommendations on how to best mitigate the threat. In December 2016, the working group, with DHS's participation, prepared a risk assessment that included information about SS7 attacks bad actors may utilize. The working group deemed this information so sensitive that it was redacted from the final report pursuant to a non-disclosure agreement. In March 2017, the working group released a public report with recommendations for best practices to reduce SS7 security risks.[2] Together, the industry publicly committed to implementing the recommendations of the CSRIC.[3]

[2] *Id.*

[3] https://www.ctia.org/docs/default-source/default-document-library/ss7-statement-2017-final.pdf.

Our engagement with DHS on SS7 goes well beyond the CSRIC working group. We have had ongoing meetings with DHS concerning the SS7 threat before, during and after the working group's existence. We have met with DHS both as an industry (through CTIA) and individually. In these meetings, we have shared specific, confidential information concerning our knowledge of known SS7 threats and the specific actions AT&T is taking (and plans to take) to address those threats, including the filtering techniques and other technical capabilities we have placed into our network. We have also updated DHS as we have implemented the GSMA best practices. We have provided your staff similar information and, as noted, would be willing to update them in an appropriate, confidential setting.[4]

We appreciate and share your interest in protecting the SS7 network from malicious actors. If you or your staff has any further questions, please do not hesitate to contact me.

Sincerely,

[4] You ask hypothetical questions concerning our interaction with DHS on testing of AT&T's network. To the extent DHS has questions or requests information regarding testing of our network, we stand ready to respond to DHS directly.