



Frontier Airlines, Inc.  
P.O. Box 492085  
Denver, CO 80249-7312

January 4, 2016

The Honorable Edward Markey  
U.S. Senate Committee on Commerce,  
Science and Transportation and Subcommittee  
on Aviation Operations, Safety and Security  
Washington, DC 20510-6125

Dear Senator Markey:

Thank you for your letter of December 2, 2015, and for allowing us an opportunity to respond. We appreciate your concern with aviation safety. Our business model is centered on this premise.

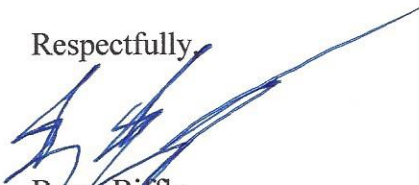
#### QUESTION RESPONSES:

- 1) We have no equipment onboard our 100% Airbus fleet which is easily susceptible to cyberattack. Each manufacturer-provided system is proprietary and closed-loop, and contains no integration with open systems. In addition, Airbus has robust cybersecurity systems and procedures in place which it continually reviews to ensure protection against potential cyberattacks.
- 2) We have not installed, nor do we have plans to install, communications that will allow passengers to use in-flight wireless services.
- 3) We ensure that cyber-threats in non-critical systems do not penetrate or compromise our on-board flight critical systems by prohibiting uploading of data to the aircraft with the exception of navigation data (NavData). Jeppesen is the proprietary manufacturer of password-protected NavData, which is monthly uploaded into each aircraft via disk by trained maintenance personnel. The lack of an inflight entertainment system, coupled with closed-loop on-board avionics, prevents passengers from penetrating our flight-critical systems. As the industry transitions to NextGen, we will carefully analyze associated new technology to ensure proper cybersecurity measures are implemented.
- 4) Cybersecurity tests on our planes' computer systems are conducted at a software/hardware certification level by the original equipment manufacturers.
- 5) As mentioned in response 3) above, the only computer software updates installed on our aircraft are for NavData. NavData installation is performed either by Company maintenance personnel or third-party maintenance providers. We require security background checks both for our employees and for those of our third-party providers.

- 6) We are not aware of any instances of infiltration, efforts to infiltrate, or intentional or inadvertent introduction of malicious code, with respect to any of Frontier's computer systems or aircraft systems in the past five years.
- 7) Frontier has a comprehensive cybersecurity policy that focuses on prevention, monitoring and responding to cybersecurity threats. Customer flight data is stored by Navitaire, a third-party reservation system provider, in its private data centers. Both Frontier and Navitaire encrypt, firewall, and monitor access to customer flight data. Both companies also remove certain personal identifying information and store and circulate data on a need-to-know basis. Aside from Navitaire, we do not share customer data with third parties.
- 8) We have not collaborated with any government agencies to prevent cyber-threats. We do, however, comply with all legal and regulatory requirements in this area. In addition, we have collaborated with Airbus to understand its cybersecurity measures, as it is the type certificate holder for all of our aircraft.

Please contact me if you require any additional information.

Respectfully



Barry Biffle  
President