Response to Written Questions Submitted by Chairman John Thune to Karen Zacharia

Question 1. Regarding the 2013 and 2014 breaches, Yahoo! has pointed out that the stolen information did not include social security numbers, clear text passwords, or other sensitive financial information. Nevertheless, the account information that was compromised did include information that could be used to access sensitive information. Consumers have been known to e-mail personal information, password reminders, as well as other sensitive details to themselves or others. And while Yahoo! took action around the time of its announcements to protect its user accounts, at least with respect to the 2013 breach, there was a three-year window during which these accounts were unprotected. Does Verizon have any evidence showing that consumers were exposed to higher risk based on information subsequently accessed from user accounts using stolen credentials? If so, please provide this evidence.

Response. Verizon has no evidence that the data elements taken by the intruders in the 2013 and 2014 data thefts—including names, email addresses, telephone numbers, dates of birth, hashed passwords and encrypted or unencrypted security questions and answers—resulted in access and use of information in consumers' email content to perpetrate identity theft or financial fraud. Yahoo has received complaints (e.g., via Yahoo Customer Care and civil lawsuits arising from the 2013 and 2014 data thefts), some of which allege that harm has occurred as a result of the 2013 and 2014 data thefts. However, these claims have not been substantiated or causally connected to the data thefts. In addition, Yahoo's systems would trigger additional verification requirements, including a second login challenge, that would provide security for accounts beyond the users' hashed passwords (which were not taken in clear text in either incident). Yahoo also has taken additional steps to enhance user security, including the strengthening of internal controls and a forced password reset for users. Yahoo also has encouraged users to adopt key-based authentication in lieu of passwords.

Further, as the Department of Justice stated in a press release, one of four state sponsored hackers who was indicted for the criminal intrusions "exploited his access to Yahoo's network for his personal financial gain, by searching Yahoo user communications for credit card and gift card numbers. . . ." Dept. of Justice, Office of Public Affairs, U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts, March 15, 2017, at p. 1. We have no evidence, however, that the content of any of the user communications referenced in the press release were used to perpetrate identity theft or resulted in financial fraud.

Question 2. Does Verizon support the enactment of a single federal breach notification standard? If so, what form should it take?

Response. Yes, Verizon supports enactment of a Federal breach notification law that would set a national standard. This would provide consumers across the country with consistent notices and will lead to a greater understanding by consumers about why they are being notified and what actions might be appropriate for them to take. The following two elements are particularly important to include in a Federal breach notification law: (a) mandating notices in the appropriate circumstances, such as when there is a material risk of identity theft or financial fraud, thus avoiding over-notification which desensitizes consumers to the notices they receive; and (b) preempting the existing state patchwork framework that currently exists which leads to consumer confusion.