Responses to Written Questions Submitted by Chairman John Thune to Paulino do Rego Barros, Jr

Question 1. On October 6, Equifax advised the Committee that it would send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. It also advised that it would mail written notices to all of the additional potentially impacted U.S. consumers – about 2.5 million – identified since the September 7 announcement. Please provide an update on the status of these notices, including what challenges Equifax has faced in attempting to comply with 52 separate data breach notification laws.

Response. Equifax has completed mailing written notices to the three populations identified above. While the 52 separate data breach notification laws generally require notice to be sent to residents when a consumer's personal information is acquired in an unauthorized manner that compromises the security or confidentiality of that information, statutes vary with regard to several aspects of the breach notification requirements.

Generally, the most significant differences to reconcile include the threshold for issuing a substitute notice versus a direct notice, the required timing and content of the notification, regulator notices, and the definition of personally identifiable information ("PII").

While most states have the same general content requirements, some states have specific content requirements that typically require separate form notification letters in order to comply. As a result, the information consumers receive about a multi-state incident may differ depending on where they reside and the requirements of their states. For example, California requires specific titles and headings, Massachusetts notifications cannot include information about the nature of the breach or the number of affected individuals, and Maryland and North Carolina require that state-specific Attorney General contact information be included in notices to their residents.

Notable variances in state breach notification statutes ultimately result in varying levels of information being provided to consumers and regulators depending on their state's specific requirements.

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

Response. Yes. A single federal breach notification standard would help ensure that all impacted consumers and regulators receive the same information regarding a breach incident in an efficient and expedient manner. Lawmakers may want to consider key elements in developing a federal standard including:

Direct and Substitute Notices: All state statutes provide for a substitute or alternate notice versus a direct notice to consumers depending on the cost of a direct notice, the universe of affected consumers residing in the state, or the lack of sufficient contact information for the consumers. States agree that flexibility is important when considering notification, and that all breach incidents should not necessarily require a direct notification to all impacted consumers.

Timing: Many states require notification "in the most expedient time and manner possible and without unreasonable delay" following the discovery of a breach (for example, New York and

California data breach statutes). This guidance allows the breached entity time to determine the scope of the incident and the number of consumers impacted, and to restore the integrity of systems before moving forward with public notification. While a minority of states require notice within a specific time frame, generally between 30 to 45 days, most states recognize that it is important for a breached entity to conduct an investigation and to complete corrective actions before providing notification. This will help ensure that the security or technological vulnerability has been addressed and the breach notification is provided to the correct consumers and includes the most accurate information regarding the incident.

Content Notification: Most states have the same general content requirements and allow for a breached entity to provide a "standard" letter to a majority of impacted consumers that includes the date of the breach; a general description of the incident; the type of PII impacted; contact information for the breached entity; contact information for the consumer reporting agencies, the Federal Trade Commission and Attorneys General; steps taken to prevent a further breach; and advice to consumers regarding protecting against identity theft. Some states, however, have state-specific requirements that require separate form notification letters, as noted in the response above. Consistent content notification requirements across all states would ensure that consumers receive the same information regarding a breach incident regardless of where they reside. Further, the breached entity would likely be able to make the disclosure more quickly and efficiently, to the benefit of consumers.

Regulator Notices & Enforcement: Some states require notice be provided to the state's Attorney General or other state regulators. A federal breach law may want to consider consolidating regulator notices to a single federal authority to streamline the initial notification, centralize follow-up requests and information regarding the incident, coordinate communication among various stakeholders, and, ultimately, enforce a federal breach notification standard.

Other provisions to consider when evaluating a federal breach notification standard should include whether PII is "acquired" versus "accessed," whether the breached entity is a "data owner" versus a "maintainer," the definition of PII, a risk-of-harm analysis, data encryption, and "electronic" versus "paper records."

Question 3. On October 6, Equifax advised the Committee that it is in the process of contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulator inquiries. Please provide an update on the status of Equifax's efforts to contact U.S. state and federal regulators regarding the breach.

Response. Equifax notified the Federal Bureau of Investigation ("FBI") about the incident in question on August 2, 2017. Equifax notified the Federal Trade Commission ("FTC") and the Consumer Financial Protection Bureau ("CFPB") via phone calls on September 7, 2017, at approximately the same time Equifax published its official press release announcing the cybersecurity incident. In addition, Equifax provided written notifications to 52 state attorneys general on September 7, 2017. Upon the completion of the forensic investigation, Equifax also provided supplemental notifications to those 52 state attorneys general on October 12, 2017. We

continue to cooperate with these regulators and law enforcement agencies, among others, in connection with the cybersecurity incident.

Question 4. At the time of the data breach, was Equifax in compliance with the FTC Safeguards Rule? If so, do you believe the fact that the data breach occurred signals that the rule should be strengthened?

Response. Data security and integrity are of paramount importance to Equifax. Equifax has a formalized security program supported by administrative, technical, and physical safeguards focused on the protection of consumer data. Equifax has a security team in place that is responsible for the coordination and execution of the Company's information security program. The security team reports to Equifax's Chief Security Officer, who reports directly to Equifax's CEO, and operates using defined plans and procedures for responding to security incidents, which are revised on a regular basis. Security incidents are classified according to severity and escalated to management personnel as appropriate. The security team includes dedicated incident response managers and a Cyber Threat Center, which is staffed by security professionals and uses technological capabilities to monitor the Company's network. Equifax has physical safeguards in place to secure its data centers. The data security incident that Equifax disclosed on September 7, 2017, does not by itself suggest that the Safeguards Rule needs revision. Equifax will be better informed to make regulatory and legislative observations after the internal and external reviews of the incident have been completed.

Question 5. What specific steps has Equifax taken to comply with the Safeguards Rule since it discovered the data breach?

Response. Equifax is conducting a root cause investigation related to the incident announced on September 7, 2017 and is dedicated to resolving any issues identified as a result of that investigation. Moreover, Equifax has already made important improvements to its data security infrastructure. It is further hardening its networks, changing its procedures to require "closed loop" confirmation when software patches are applied, rolling out new vulnerability detection tools, and strengthening accountability mechanisms. Equifax has implemented certain technological remediation steps as described in the Mandiant executive summary, which was submitted to this Committee on September 25, 2017. Equifax has also engaged PwC to help identify and implement a security program transformation, including tactical immediate changes, strategic remediation, and operational improvement initiatives that will allow the Company to strengthen its long-term data protection and cybersecurity posture.

Question 6. Does Equifax have any evidence showing that consumers have experienced identity theft or other harm as a result of the data breach? If so, please provide this evidence.

Response. Equifax has not seen evidence that consumers have experienced identity theft or other financial harm as a result of the cybersecurity incident.

Question 7. Has Equifax identified any of the hackers or other persons or entities that obtained consumer information from the company in connection with the data breach?

Response. Equifax is conducting an internal investigation into this incident and continues to work closely with the FBI in the FBI's investigation into this matter. At this time, Equifax is not aware that the perpetrators have been identified.

Responses to Written Questions Submitted by Honorable Dean Heller to Paulino do Rego Barros, Jr

Question 1. Protecting data isn't just about the Internet—it's also about the physical security of data. In my home state of Nevada, we have the only Tier 5 rated data centers in the world. The best security and reliability you can get from a data center. What standards are you following to ensure that the data you manage is physically secure?

Response. All Equifax facilities, including owned and operated data centers, are governed by the Equifax Corporate Security Policy and the Equifax Physical Security Tier Standard. Under the company's standard, Equifax data centers and data storage facilities are classified as "Tier 1 – Critical Operations Facilities" and have the most stringent physical security requirements, including among others:

Security Intrusion Detection Systems and 24x7 Monitoring;

Man traps;

Electronic access control systems;

Minimum two-factor authentication;

Formal access provisioning including formal visitor logs;

Cameras monitoring access points; and

Security guards.

In addition, Equifax performs annual Physical Security Surveys of data centers, which include assessments of the effectiveness and completeness of the controls in place based on identified risks to the data center and the requirements of the Equifax Physical Security Tier Standard. Equifax also performs preventative maintenance and testing of all electronic physical controls.