EQUIFAX'S SUBMISSION IN RESPONSE TO SUBCOMMITTEE REQUESTS DATED OCTOBER 11, 2017

Each question is copied below for reference, although certain introductory statements are omitted.

QUESTIONS FOR THE RECORD FOR RICHARD SMITH, FORMER CEO, EQUIFAX, SUBMITTED BY SENATOR PATRICK LEAHY

Sen. Leahy Question #1. Why did Equifax not have the systems in place—and back-up systems if need be—to immediately act on the March 8th security alert, which was more than two months before the data breach began?

Response: On March 9, 2017, Equifax disseminated the U.S. Department of Homeland Security, Computer Emergency Readiness Team ("U.S. CERT") notification internally by email requesting that applicable personnel responsible for an Apache Struts installation upgrade their software. Consistent with Equifax's existing patching policy, the Equifax security department required that patching occur within a 48 hour time period. Equifax now knows that the vulnerable version of Apache Struts within Equifax was not identified or patched in response to the internal March 9 notification to information technology personnel.

On March 15, 2017, Equifax's information security department ran scans that should have identified any systems that were vulnerable to the Apache Struts issue identified by U.S. CERT. Unfortunately, however, the scans did not identify the Apache Struts vulnerability. Equifax's efforts undertaken in March 2017 did not identify any versions of Apache Struts that were subject to this vulnerability.

In sum, the breach occurred because of both human error and technology failures. These mistakes were made in the same chain of security systems designed with redundancies.

Equifax has implemented several updates to protocols and procedures in response to this incident. Vulnerability scanning and patch management processes and procedures have been enhanced. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies on application and web servers has been accelerated. The company is also implementing additional network, application, database, and system-level

logging. These are just a few of the steps Equifax has taken since the breach was discovered to shore up its security protocols.

Equifax's forensic consultants have recommended and are implementing a series of improvements that are being installed over 30, 60, and 90 day periods. Equifax also engaged PwC to assist with its security program, including strategic remediation and transformation initiatives that will help Equifax identify and implement solutions to strengthen its long-term data protection and cyber security posture.

Beyond the technological enhancements, Equifax has also made several strategic personnel changes at the highest levels of the company since September 7, 2017. The CEO stepped down and the Chief Information Officer and Chief Security Officer also resigned from their positions.

Sen. Leahy Question #2a. Why did it take nearly six weeks from the date Equifax discovered the breach to the date that Equifax finally disclosed the breach to consumers and to regulators?

Response: Between August and September 2017, Equifax acted with diligence to secure and diagnosis the suspicious activity observed on July 29 and 30. On August 2, consistent with its security incident response procedures, the Company (1) retained the cybersecurity group at the law firm of King & Spalding LLP to guide the investigation and provide legal and regulatory advice; (2) engaged, through company counsel, the independent cybersecurity forensic firm, Mandiant, to investigate the suspicious activity; and (3) contacted the Federal Bureau of Investigation ("FBI"). It was not until well into August that Mandiant understood the scope of the consumer data impacted by the incident. Over the next several weeks, Mandiant and Equifax's security department analyzed forensic data seeking to identify and understand these early indications of unauthorized activity on the network. Their task was to figure out what happened, what parts of the Equifax network were affected, identify consumers that were impacted, and what information was accessed or potentially acquired by the hackers. This effort included identifying and analyzing available forensic data to assess the attacker activity, determining the scope of the intrusion, and assessing whether the intrusion was ongoing (it was not; it had stopped on July 30, when the portal was taken offline). Mandiant also helped examine whether the data accessed contained personal identifying information ("PII"), discover what data was exfiltrated from the company, and trace that data back to unique consumer information.

By September 4, the investigative team had created a list of approximately 143 million consumers whose personal information was believed to have been impacted, and Equifax continued its planning for a public announcement of a breach of that magnitude, which included a rollout of a comprehensive support package for consumers. The team continued its work on a dedicated website, www.equifaxsecurity2017.com, where consumers could learn whether they were

impacted and find out more information, a dedicated call center to assist consumers with questions, and a free credit file monitoring and identity theft protection package for all U.S. consumers, regardless of whether they were impacted.

Equifax kept the FBI informed of the progress and significant developments in our investigation, and felt it was important to notify the FBI before moving forward with any public announcement. The company notified the FBI in advance of the impending notification.

On September 7, 2017, Equifax provided notification of the incident by issuing a nationwide press release, providing the dedicated website where consumers could determine if they were impacted and sign up for the credit file monitoring and identity theft protection product, and providing a dedicated call center for consumers. The notification indicated that the incident impacted personal information relating to approximately 143 million U.S. consumers, primarily including names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. On October 2, 2017, following the completion of the forensic portion of the investigation of the incident, Equifax announced that approximately 2.5 million additional U.S. consumers were potentially impacted, for a total of 145.5 million.

Sen. Leahy Question #2b. What risks were there to consumers' sensitive personal information in the meantime?

Response: On September 7, 2017, Equifax publicly announced that the breach impacted personal information primarily including names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. Credit card numbers and information contained on dispute documents were also impacted for some consumers.

Mandiant, a leading independent cybersecurity firm, was engaged to investigate this incident. Mandiant has provided Equifax with an executive summary, a supplemental report, and a final supplement, which were supplied to the Subcommittee on October 1 (executive summary and supplemental report) and October 6 (final supplement). These materials also provide information about the consumer data that was accessed.

We believe that the best way for consumers to protect themselves and prevent any harm from occurring as a result of the incident is to enroll in TrustedID Premier and utilize the free lock product beginning in January.

Sen. Leahy Question #3. Do you still believe that stronger cybersecurity and notice requirements are unnecessary in your industry?

Response: Equifax did not lobby against the Consumer Privacy Protections Act, nor did Equifax lobby in support or opposition of any cybersecurity legislation in the 114th Congress. Cybersecurity is an important issue to the credit data industry

and Equifax listed the bill on the Equifax Lobbying Report because the company appropriately monitors legislation that impacts their business and was attempting to be transparent regarding its interest.

Equifax supports efforts to protect the public's personal and private information, and is happy to engage with Congress about the specific details of any proposed legislation that would help achieve that goal. Equifax has provided observations regarding cybersecurity protections and notice requirements to other committees and would be happy to share those observations with your office.

Sen. Leahy Question #4. Would the possibility of consumers protecting their rights through litigation create an incentive for companies like Equifax to take additional steps to protect consumers' sensitive personal information?

Response: Equifax is taking a variety of steps to help protect consumers' sensitive personal information. Please see responses to Senator Coons questions #2b, #3, and #4 for just a few examples.

Equifax would be happy to discuss with your office the various state-law systems, how they work, and the best way to protect consumers in the most effective manner.

QUESTIONS FOR THE RECORD FOR RICHARD SMITH, FORMER CEO, EQUIFAX, SUBMITTED BY SENATOR CHRISTOPHER COONS

Sen. Coons Question #1. On March 8, 2017, the Department of Homeland Security alerted Equifax to a software vulnerability. The next day, an Equifax security team was directed to install a routine patch which would solve the vulnerability. That did not occur, and this vulnerability led to the breach, which was not discovered for months. What procedures should be put in place to ensure that adequate cybersecurity does not depend on a chain of communication and execution that may be broken by one person's failure?

Response: The breach occurred because of both human error and technology failures. These mistakes were made in the same chain of security systems designed with redundancies.

Equifax has implemented several updates to protocols and procedures in response to this incident. Vulnerability scanning and patch management processes and procedures have been enhanced, including an improvement to Equifax's patching procedures to require a "closed loop" confirmation, which is applied to necessary patches. The scope of sensitive data retained in backend databases has been reduced so as to minimize the risk of loss. Restrictions and controls for accessing data housed within critical databases have been strengthened. Network segmentation has been increased to restrict access from internet facing systems to backend databases and data stores. Additional web application firewalls have been deployed, and tuning signatures designed to block attacks have been added. Deployment of file integrity monitoring technologies on application and web servers has been accelerated. The Company is also implementing additional network, application, database, and system-level logging. These are just a few of the steps Equifax has taken since the breach was discovered to shore up its security protocols.

Equifax's forensic consultants have recommended and are implementing a series of improvements that are being installed over 30, 60, and 90 day periods. Equifax also engaged PwC to assist with its security program, including strategic remediation and transformation initiatives that will help Equifax identify and implement solutions to strengthen its long-term data protection and cyber security posture.

Beyond the technological enhancements, Equifax has also made several strategic personnel changes at the highest levels of the company since September 7, 2017. The CEO stepped down and the Chief Information Officer and Chief Security Officer also resigned from their positions.

Sen. Coons Question #2a. One proposal suggested at the hearing would be to require a credit reporting agency to institute automatic credit freezes when the agency detects a breach. What are the pros and cons of a federal law mandating credit freezes in such situations?

Response: Various stakeholders, from consumer groups to financial institutions to credit bureaus, recognize that a credit freeze creates a deliberate hurdle for a consumer—or a fraudster—to gain access to credit. Federal law—and applicable state laws—has long held that the decision to impose a freeze should be at the direction of the consumer. Equifax would be reluctant to impose an automatic credit freeze in any circumstance, particularly without the consumer's knowledge. Some Members and Committees in the current Congress are considering changes to federal law to unify and simplify the processes to secure a credit freeze, including consideration of preemption of relevant state freeze laws.

Sen. Coons Question #2b. Do you believe it would be advantageous to make it easier for consumers to freeze and unfreeze their credit? Why or why not?

Response: Equifax has implemented a suite of products to assist consumers with freezing and unfreezing their credit, as well as features for locking and unlocking consumer credit files.

At the most basic level, a credit file lock and a security freeze do the same thing: they both help prevent creditors and other lenders from accessing your Equifax credit file, with certain exceptions. Unless a consumer gives permission or takes an action, such as removing, unlocking or lifting the freeze or lock, a lender or other creditor cannot access the consumer's Equifax credit report with a security freeze or a credit file lock in place.

Security freezes (also known as credit freezes) were created in the early 2000's, are subject to regulation by each state, and use a PIN based system for identity authentication. Credit file locks were created more recently, are mobile-enabled, and use modern identity authentication techniques, such as username and passwords and one time passcodes for better user experience.

Detailed directions for freezing or locking an Equifax credit file are set forth on the company's website. The directions are paraphrased below:

> **Lock** – To lock your Equifax credit file, enroll in TrustedID Premier. This credit file monitoring and identity theft protection product is free for one year to all U.S. consumers who enroll by January 31, 2018. Once you have finalized your activation in TrustedID Premier, visit www.trustedid.com, login and simply click the lock button. There are some exceptions where a lock may be delayed or may not be possible. Once you have finalized your activation in TrustedID Premier, visit www.trustedid.com, login, and simply click the lock button.
>
> To unlock an Equifax credit file, once you have finalized your activation in TrustedID Premier, visit www.trustedid.com, log in and simply click the unlock button.

Freeze – An Equifax security freeze can be placed by mail, phone, or online. Equifax has waived the fee to add, lift, or permanently remove a security freeze on Equifax credit files through January 31, 2018. Any freeze activities after January 31, 2018 may be subject to the fees provided by your state of residence. The easiest and fastest way to freeze your Equifax credit file is by using Equifax's online process found at the following link: www.freeze.equifax.com. If you choose, you may also request a security freeze by calling Equifax's automated line at 1-800-685-1111. NY residents please call 1-800-349-9960. You may also submit your request in writing to:

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348

When you freeze your Equifax credit file, you will receive a 10-digit randomly generated PIN from Equifax that you will need to save and have available should you choose to temporarily lift or permanently remove the freeze in the future.

Sen. Coons Question #3. One of the great threats emerging from this breach is that the hackers have permanent identifying information for American consumers who do not know whether their information was stolen. Beyond temporary credit freezes, what can consumers do to protect themselves?

Response: In response to the cybersecurity incident, Equifax developed a robust package of remedial protections for each and every American consumer—not just those affected by the breach—to protect their credit information. The relief package includes (1) monitoring of consumer credit files across all three bureaus, (2) access to Equifax credit files, (3) the ability to lock the Equifax credit file, (4) an insurance policy to cover out-of-pocket costs associated with identity theft, and (5) dark web scans for consumers' social security numbers. All five of these services are free and without cost to all Americans.

Equifax has also taken steps to better protect consumer data moving forward. The Company announced a new service that will be available by January 31, 2018, that will allow consumers to control their own credit data, by allowing them to lock and unlock their credit files at will, repeatedly, for free, for life.

Finally, in addition to the services described above, security freezes, and fraud alerts are available to consumers to help protect against credit fraud.

Sen. Coons Question #4. In January 2017, I introduced S. Res 23, which would establish a new, permanent Senate Select Committee on Cybersecurity to give Congress the tools to comprehensively investigate and respond to cyber intrusions, take proactive steps to protect against and respond to future attacks, and provide oversight of government

agencies. What steps do you recommend to increase public-sector and private-sector cooperation to enhance the security of consumer data?

Response: The public and private sectors can both benefit from working together on cybersecurity initiatives. To improve public-private cybersecurity cooperation, the government may want to consider establishing an environment where companies can voluntarily engage with regulators in a setting based on cooperative engagement without the risk of punitive enforcement. Creating a limited safe harbor for private entities to share with regulators, would encourage companies to participate. Congress may also want to consider whether the federal agencies engaged in a potential public-private partnership can appropriately distinguish their engagement from their roles as enforcement agencies.

Sen. Coons Question #5. At the hearing, several members of the Judiciary Committee asked questions related to using authentication systems other than social security numbers. Which alternative authentication systems do you believe are the most important alternatives to consider and why?

Response: The U.S. should consider moving to a dynamic system of personal identity, one built on a multi-factor authentication system that includes a dynamic or constantly changing identifier, such as consumer transaction data or one-time SMS verification codes. The problem with identity theft is not the Social Security number ("SSN"); it is that SSNs are used for things they were never intended for, such as authenticating a consumer's identity. Instead of trying to replace SSNs, Congress should consider augmenting them, similar to how multi-factor authentication systems build on existing password authentication. This means treating a SSN as only one piece of verifying a consumer's identity and asking them for additional private information as well, such as what were the consumer's last three transactions on their bank card or a one-time code provided to the consumer at a confirmed phone number. Relying solely on a SSN as a form of authentication is not a good practice, nor has it been a standard industry practice for many years.

Sen. Coons Question #6. Following the breach, Equifax offered a free one-year membership in their Trusted ID Premier consumer protection product for consumers that sign up by January 31, 2018. The membership agreement, however, contained a binding arbitration clause, forcing consumers to waive their right to hold Equifax accountable in court. During your hearing before the Senate Banking Committee, you asserted that the presence of the arbitration clause was a "mistake" and was removed as soon as possible. Do you agree that it would be unfair to apply a binding arbitration clause to a consumer who enrolled in the Trusted ID Premier consumer protection product as a result of the data breach?

Response: Equifax immediately addressed confusion concerning the arbitration and class-action waiver clauses initially included in the Terms of Use applicable to TrustedID products. Equifax never intended to prohibit or limit any consumers' right to take legal action in connection with the breach. The company

immediately updated its terms and conditions on the website and on the TrustedID Premier program to make that clear. The company clarified that the clauses will not apply to consumers who signed up before the language was removed. To be as clear as possible, Equifax will not apply any arbitration clause or class action waiver against consumers for claims related to the free tools offered in response to the cybersecurity incident or for claims related to the cybersecurity incident itself.

* * *