Professor Tyler Moore – Equifax: Continuing to Monitor Data-Broker Cybersecurity
Questions for the Record
Submitted October 11, 2017
Responded October 25, 2017

Questions from Senator Coons

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?

The NIST cybersecurity framework outlines a series of controls that organizations can adopt to improve their cybersecurity. The "identify" and "detect" controls, if adequately implemented, should help avoid a similar series of compounding failures to take hold in future.

Ultimately, though, success in defending against attacks such as these requires that the defender internalize the costs of insecurity as much as possible. This would encourage firms to adequately invest in cybersecurity defenses commensurate to the threats they face.

2. 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.
    a. What are the pros and cons of a federal law mandating credit freezes in such situations?
    b. Do you believe it would be advantageous to make it easier for consumers to freeze and unfreeze their credit? Why or why not?

In my testimony, I advocated for credit reporting agencies to freeze consumer credit by default, as outlined in your question. There are two key advantages to mandatory freezes following a data breach like the one Equifax experienced. First, it is the only adequate defense when the stolen data is all that's required to fraudulently open new credit accounts. Second, it would strongly incentivize the credit reporting agencies to innovate and come up with easy-to-use and reliable mechanisms to unfreeze credit.

This is important because the main disadvantage to freezing credit today is that it is burdensome to unfreeze. But most of these burdens can easily be overcome. For example, eliminating fees for freezing and unfreezing credit is a policy decision any credit reporting agency can make (as illustrated by Equifax having already done so, at least temporarily). Making it easier for consumers to freeze and unfreeze their credit matters because ensuring widespread access to credit is hugely important for our economy.

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?

Unfortunately, the harms arising from this breach are so substantial and persistent that the defensive steps consumers can take only provide incomplete protection. There's not much consumers can do beyond freezing credit to protect themselves. One step that consumers can and should be encouraged to take is to report any instance of fraud, harassment or other abuse to their local police. This step will help policymakers better quantify the resulting harms, but it also can help protect consumers by creating lasting evidence of the fraud if they experience even more fraud many years later.

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?

Taking a holistic approach to cybersecurity policy is essential, as it is an issue that spans many industries, jurisdictions and purviews.

The public sector can play an essential coordinating role in gathering, aggregating and disseminating data on harms that arise from data breaches. Right now, firms are only obliged to disclose that a breach of personal information has occurred. They are not required to share information on resulting harms, such as increased fraud or customer disputes that result from breaches. Firms should be encouraged to share such information voluntarily, but if they do not, then compulsory disclosure may be required. By gathering and sharing information on the prevalence and cost of harms, firms can elect to devote adequate resources commensurate to the threat.

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?

The particular technology of the alternative authentication mechanism is not so important. What is essential is that authentication not be based on public information that cannot be changed, as is the case with Social Security numbers. The simplest authentication mechanism would be to use passwords that can be more easily updated in the event of a breach. Some form of two-factor authentication would be preferred, complementing something you know (e.g., a password) with something you have (e.g., a hardware token or a smartphone receiving a one-time SMS code) or something you are (e.g., biometrics). It would be preferable to support multiple forms of authentication, rather than a single monolithic approach. The key is to move away from authenticating based on public and widely compromised information (i.e., the Social Security number).

6. At the hearing, every witness agreed that the Equifax data breach has created national security risks. With detailed information on government employees with security clearances, foreign powers or private actors could target Americans and attempt to obtain

access to classified information. What immediate and long-term steps do you recommend that the government take to minimize these security threats?

Unfortunately, there is no countermeasure available to the government that can completely mitigate the resulting national security risk. One option is to proactively monitor for attempts to exploit the stolen information. Another is to conduct reviews of employees with security clearances to identify those who are at elevated risk of targeting (e.g., have access to top secret information and could have potentially compromising information in their credit report).

7. Ant Financial, an affiliate of the Chinese company Alibaba, has made attempts to acquire MoneyGram, raising concerns about the company's record for protecting customer data, ties to Chinese authorities, and data warehousing. Is extra scrutiny warranted to ensure that this acquisition comports with national security interests?