Professor Jamie Winterton – Equifax: Continuing to Monitor Data-Broker Cybersecurity
Questions for the Record
Submitted October 11, 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?

During the hearing, the former CEO of Equifax argued that the breach was in part due to "human error" – that an individual on the security team did not install a patch or communicate clearly which patch should be installed. I disagree. This is not an error at the human level, but an error at a leadership and an organizational level. For a single individual to be responsible for Equifax's patch management shows an institutional lack of concern for security and lack of respect for the people whose data they maintained.

Patching isn't trivial, but it's possibly the most important piece of a company's security posture. Understanding the network is key – which segments can be easily patched, and which have legacy software that may be problematic to update. Those legacy pieces should be isolated from the rest of the network and specifically monitored until an appropriate patch method is identified. Patching speed is key – a 60-day or even 30-day patch cycle often isn't sufficient if an asset may be exposed directly to external attacks, particularly when malicious campaigns or proof-of-concept attacks are known to be exploiting the vulnerability. Some organizations have implemented weekly or daily patching procedures for critical vulnerabilities in exposed systems. The organization's systems should also be subject to regular, consistent monitoring and review – if a patch is available but not installed, that problem should be discovered promptly, elevated, and the risks assessed accordingly. Patching isn't just an IT problem; it has organizational-level impacts on compliance as well as operational efficiency – so the patch strategy, with its benefits and risks, should be well understood at the C-suite level.

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?

Consumers attempting to freeze their credit were incredibly frustrated in the weeks following the Equifax disclosure. The infrastructure didn't exist to handle the volume of calls, the website required too much information from consumers, and once consumers froze their credit with one agency, they had two more agencies to approach. Automatically freezing credit – in the case of a breach or just as general practice – would relieve the burden on the consumer. Implementation of an automatic credit freeze may be difficult – these policies would have to be enacted quickly on a large scale. Also, if a breach occurs while a consumer is in the middle of a time-sensitive transaction – buying a house, for example – a method to quickly thaw their credit will be important.

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

It would certainly be advantageous for consumers. Most people only need to use their credit when

they're applying for new financing – that doesn't happen often. Consumers should be empowered to decide when their credit is available, instead of having it available continually. They should be able to freeze their credit easily with all three agencies, and unfreeze it just as easily. Identity theft would be less appealing to criminals if credit was frozen by default.

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?

The day before our hearing, the number of records lost in the Equifax breach was revised upwards, from 143.5M to 145M. The same day, Yahoo revised its breach number from 1B to 3B. Many other victims of large-scale breaches have also discovered after their initial notification that more records were exposed than previously thought. Given that, it would be wise for all consumers to assume that their data has been breached, and respond accordingly. This includes initiating a credit freeze, changing passwords (especially if they have been used for multiple accounts), and examining their credit history for suspicious activity. As general security measures, I recommend using two-factor authentication on accounts, whenever available, and employing a password manager to help create and manage robust passwords that differ for each account.

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?

Public/private partnerships are a critical part of situational awareness in cybersecurity. Before they participate, companies want to know that the threat intelligence they're providing from their own networks won't be used against them – that it won't expose information that would provide an advantage to their competitors, and that it won't be used to punish them. Establishing a trusted neutral third-party to obfuscate the data while maintaining its intelligence value and providing situational awareness helps incentivize private-sector participation. Companies also want to know that the indicators they receive are timely and are keeping them in front of the threat. For best value for all participants, these alliances can and should educate about best practices in security, in addition informing about current threats.

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?

It's clear we need a radically different approach to authentication, but I'm not sure what that is. Current methods all fall short. If we simply reissue a series of numbers, we haven't really solved the problem. I'm hesitant to recommend pure biometric data as an identifier – once someone's fingerprint or iris pattern has been stolen, they can't apply for a new one! Passwords aren't effective because machines easily crack the ones that humans can remember. This is a problem that requires a cutting-edge research agenda – I think a hybrid approach will end up being most effective, but how to combine identifying elements in the most robust way is an open question that deserves attention.

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?

So much of the discussion on the harm inflicted by breaches is at the individual level – and I certainly don't want to downplay those. But people who currently have clearances or have held them in the past are at risk in a unique way. The government should follow up with these people quickly, reminding them of their exceptional position and how to recognize and rebut potential targeting. Agencies and departments should collaborate to identify and implement additional measures to ensure that a targeted individual will feel supported and confident in reporting coercion and blackmail attempts to their sponsoring organizations.

In the case of Equifax, that data has already been exfiltrated and is likely in use. We need to also look forward and think about how to stop other large-scale breaches that could add to the already considerable intelligence value of exposed US data. Which sources would be the most valuable to a foreign adversary? Let's identify potential targets and work closely with them on security, both their current security posture and their long-term outlook. We shouldn't wait until we've mastered the basics to stat working on stronger, more resilient networks.

7. In your opening statement, you noted that aggregating data for 145 million people provides a detailed look at the American economy and society, including its weaknesses and vulnerabilities. How is the loss of this data a national security threat when considered in the aggregate?

145M credit records are about half the population of the United States. Credit records go back for years, showing histories of account balances, when they were opened and closed, when payments were made on time and when they were late. Aggregating and analyzing this data allows a foreign adversary to understand the priorities and inner workings of our society and potentially exploit them.