Securing Consumers' Credit Data in the Age of Digital Commerce

U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection

James Norton – QFR Answers

December 19, 2017

Questions from the Honorable David McKinley of West Virginia:

1. **What is the one most important thing companies like Equifax should do to enhance our confidence in their ability to keep sensitive data secure?**

   While there is no single policy or practice that will effectively ensure data security in all cases, I believe that, generally, companies like Equifax could enhance public confidence by providing greater transparency regarding their cybersecurity efforts – including whether they have established an executive level position within the company charged with developing and implementing security practices across the business. The executive would not be a lone ranger but would have the resources and authority across the business, with daily access to the CEO and senior government officials to work proactively to stay ahead of emerging cyber threats and safeguard sensitive data.

2. **What is the one most important thing Congress should do?**

   Congress should provide the necessary appropriation to enable and build a cyber infrastructure within Federal, state and local governments to establish them as reliable resource for the private sector. Too many companies lack the requisite expertise and resources to effectively tackle rapidly evolving cyber threats. Since the Federal Government as well as state and locals are dealing with many of the same challenges, they are well positioned to identify best practices (including by convening public and private stakeholders) and provide technical assistance. However, to date, cyber functions within the government have been under-resourced and tasked with overly broad mandates that leave little capacity for them to serve this critical leadership role for the private sector.

3. **Is social media becoming an increasingly effective tool for cyber criminals? In September after Equifax publicly disclosed the breach, Equifax repeatedly tweeted the wrong URL for its consumer protection website. Is that an example of cyber-criminal exploiting social media for nefarious purposes?**

   While I cannot comment about what may have caused Equifax to tweet the wrong link, I believe it is accurate to say that bad actors are making increasing use of social media, as a way to both spread malware and access

personal data. Consumers should be cognizant about sharing personally-identifiable information (like addresses, birth dates, and telephone numbers) on social media platforms and should be cautious when clicking on suspicious links, even those that have apparently been shared by known parties.

4. **What kind of new data security developments should CEOs, Chief Information Security Officers, and Chief Information Officers and indeed everyone be aware of?**

   In today's complex cyber environment, threats are changing rapidly, so it is imperative that company executives – especially those in charge of sensitive personal data – remain aware of the most up-do-date, effective security solutions. However, companies and individuals can also take additional simple, effective steps to improve data security. Companies must be diligent about training employees on their role in keeping information protected — with an emphasis on recognizing phishing and spear phishing emails that are designed to trick them into giving away credentials or installing malware. Training should also cover smart social media practices, ground rules for downloading software, and the importance of strong passwords. For individuals, comparatively simple steps – like regularly changing passwords and ensuring that security software is up to date – can meaningfully reduce the vulnerability of personal devices to cyber attacks.