Legal Lessons from the Capital One Breach

PUBLISHED ON
August 5, 2019

We are sort of numb by now to the weekly (almost daily) media reports of data breaches, but if the recent Capital One data breach seems a little different to you, you are on to something.

For starters, this breach is massive - more than 100 million customers are affected, making it among the very largest of its kind in the 10-plus year history of massive data breaches. Only breaches in 2017 at Equifax Corp. and in 2009 at Heartland Payment Systems included a larger number of records compromised.

The timeline of the latest breach is also remarkable. Consider:

- It began sometime in March 2019, compromising customer information dating back to 2005.
- An outsider first made Capital One aware of the breach on July 17.
- Capital One verified the breach on July 19 and first issued a press release regarding the breach later that day.
- The alleged hacker was arrested on July 30
- On that same day, a Washington D.C. law firm filed the first of several class-action lawsuits likely to be filed against Capital One on behalf of the millions of consumers affected by the breach.

Much more will unfold in this matter in the days and weeks to follow, but in the meantime, there are already some legal lessons to learn

- Why was Capital One retaining information dating back to 2005? In the world of cybersecurity, reducing the "attack surface" is key to an organization's data security. Most organizations understand this concept from a technical perspective and attempt to mitigate risk accordingly through its IT function. They can accomplish this in a number of ways, including reducing the amount of code running on their system, reducing entry points available to hackers or reducing or turning off unnecessary functionality. However, attack surface management includes some softer, less IT-driven factors, including policies and procedures relating to data retention. Unfortunately, many organizations are guilty of "data hoarding," and failing to establish or abide by common sense information retention policies, resulting in these organizations retaining (and, in turn, making available to hackers) far more data than necessary. Maybe we will learn that Capital One had a legitimate business purpose in retaining information that is over 15 years old. Instead, however, I'm certain we will learn that much of this data was retained far longer than its useful life. The lesson to be learned is that by establishing and abiding by a data retention policy is key to mitigating risk associated with data security.
- Did you notice that class actions lawsuits have already been filed against Capital One? One law firm led the charge by filing a suit on July 30 - within 24 hours of Capital One's press release announcing the breach. The lawsuit in question is relatively simple despite the size and expected complexity of the breach. It alleges that Capital One failed

to take "reasonable care" to secure sensitive information belonging to its customers. It further alleges that Capital One knew the risks of a security breach and did not take the proper steps to protect the personal information applicants and customers trusted it to safeguard. Evidenced by the speed by which this lawsuit was filed, the lesson to be learned is that there is now a well-established "game plan" for plaintiff's lawyer to hold organizations like Capital One accountable if they fail to protect consumers' data. Organizations must be aware of and trained on the legal duties they have to their customers' (and employees') data. They must understand the risks associated with data security and know that customers affected will be filing lawsuits quicker than ever.

• It is widely reported that Capital One's misconfigured web application used in connection with its operations hosted on the cloud with Amazon Web Services is a primary cause of the breach. This speculation shines light on the inherent risk with cloud-based services. Organizations using cloud-based services do not have control over the cloud provider's employees who are entrusted with administrative-level access to the organization's data. This is not an indictment against the use, or security, of cloud-based services, but instead a broader warning to organizations to engage in thorough due diligence of their cloud providers and to understand how the legal risk is shifted by way of the cloud service agreement. By moving operations to the cloud, an organization is, in larger respects, putting themselves at the mercy of the provider and the provider's employees.

There will be an abundance of additional lessons to learn from this breach, so please be on the lookout for further commentary from us. In the meantime, if your organization would like to discuss its own data policies and procedures, including its information retention policy and its incident response plan, or if it would like to better understand the legal risks associated with cloud-based services, please do not hesitate to contact me or any member of the Barley Snyder Cybersecurity Practice Group.

:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com