Sorting Through the Whirlwind of News on the Proposed Equifax Settlement and Capital One Breach

On July 22, 2019, the Federal Trade Commission (FTC) announced that it had reached a proposed settlement with Equifax in connection with a 2017 data breach that exposed sensitive, personal data of around 147 million people. According to the FTC's press release, the data breach included "names and dates of birth, Social Security numbers, physical addresses, and other personal information that could lead to identity theft and fraud." (See FTC press release Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach, July 22, 2019.)

Equifax agreed to pay between $575 million and $700 million in total. The Consumer Financial Protection Bureau (CFPB) will get $100 million of that in civil penalties with another $175 million going to states and territories. Only around $300 million with a possible extra $125 million will go to a "consumer fund" that will be used to compensate those affected by the breach through credit monitoring and various payments.

Checking whether your data was affected and what compensation and services you may be entitled to is fairly easy (to find out, visit www.equifaxbreachsettlement.com), but actually getting reimbursed may be tougher. You will need to provide support for your claim, and funds

can run out if there are too many claims. Some payouts will be reduced pro rata if they exceed the amount designated for them. For example, only $31 million is designated for the alternative reimbursement. If more than 248,000 people take this option, you won't get $125. The $31 million will be divided amongst everyone with a valid claim for the payment. If everyone affected chose it, you'd get less than $0.25. To learn more, read the FAQ's here; or, if you are ambitious, read the proposed settlement, itself. (In the time this article was being written, the FTC updated its site to explain that the high interest in the alternative payment would lead to consumers getting less than the $125. The option is still available, the FTC says, "but you will be disappointed with the amount you receive and you won't get free credit monitoring.")

The details of the event are evolving, but Capital One issued a statement of its understanding so far. (See https://www.capitalone.com/facts2019/ Overview and Frequently Asked Questions.) According to the statement, Capital One explained that there was an "unauthorized access" exposing the personal information of around 100 million U.S. and 6 million Canadian individuals. The actual breach occurred at the end of March; the potential vulnerability was reported to Capital One through its "Responsible Disclosure Program" on July 17; and the vulnerability was investigated and fixed by July 19. In contrast, the timeline in the Equifax incident is quite different. In its complaint, the FTC alleges Equifax received notice of a software vulnerability from the United States

Computer Emergency Readiness Team (US-CERT) in March of 2017, did not apply the patch in the months to come, and finally identified and addressed the vulnerability after suspicious activity was noticed. By then, the breach had already occurred.

What was exposed in the Capital One incident? As with the Equifax breach, some highly sensitive information. According to Capital One, this included information collected during credit card applications, “including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income.” Though Capital One reports that it encrypts its data as a standard practice, the data was de-encrypted during the breach. The company also reports using tokenization for certain fields (e.g., Social Security numbers) and says that such tokenized data was not exposed. Even so, some 140,000 Social Security numbers, 1 million (Canadian) Social Insurance numbers, and 80,000 linked bank account numbers were exposed. The good news is that Capital One currently thinks that it is “[u]nlikely that the information was used for fraud or disseminated…” by the person who accessed it, and the person believed responsible was quickly identified and apprehended.

Capital One reports that it immediately reached out to the FBI. By Monday, July 29, when the breach was announced, the FBI had arrested Paige A. Thompson in connection with the incident. (See Department Justice press release, Seattle Tech Worker Arrested for Data Theft involving Large Financial Services Company, July 29, 2019.) Thompson

allegedly accessed the data, stored on a cloud-based server, “through a misconfigured web application firewall that enabled access to the data.” Thompson allegedly posted information about accessing the data on GitHub. A user seeing it reported it to Capital One. The complaint against Thompson charged her with computer fraud and abuse. If convicted, she could face five years in prison and a $250,000 fine.

While Thompson is being widely reported as a former Amazon Web Service (AWS) software engineer, the cloud provider Capital One was apparently using, the complaint filed against Thompson does not refer to AWS by name. While the breach appears to be the result of a misconfiguration rather than a flaw in the cloud service itself, the incident has some people raising questions about cloud security more generally. In his article Capital One Breach Casts Shadow Over Cloud Security, Wall Street Journal tech reporter Robert McMillian notes that Capital One “was an early adopter of cloud-computing among financial institutions as many other banks hesitated to move customer data out of their data centers.”

In the same piece, Chris Vickery, the director of cyber-risk research and security from UpGuard, Inc., is quoted as saying “It’s easy to misconfigure things and it’s easy to have catastrophic results from those misconfigurations.” So far, that appears to be what happened here. Configuration mistakes are not uncommon, but these issues are not limited to cloud-computing. What should give us pause is that this mistake happened to a tech-savvy, fintech company like Capital One.

As the details of the Capital One breach and the investigation into Thompson continue to evolve, it is possible we will learn that other entities were also exposed. In the complaint against Thompson, the FBI says that, in addition to items related to Capital One, agents saw “files and other items” related to “other entities that may have been the targets of attempted or actual network intrusion…” (See U.S. v Thompson, Case No. MJ19-0344, July 29, 2019.)