CAPITAL ONE FINANCIAL CORPORATION'S DATA BREACH: DATA BREACH OF OVER 100 MILLION CUSTOMERS

SERGIO GUIDA

Independent Researcher, Sr.Data/Information Governance Mgr.

Key-words: data breach - hackers - cloud computing - risk management - cybersecurity

Category: Legal Area

Capital One Financial, the fifth-largest US credit card group, announced that it had suffered a hacker attack that led to the violation of personal data relating to 100 million customers in the United States and 6 million in Canada. The attack targeted customers who had submitted a request for a credit card to the Virginia-based bank or who are already customers of Capital One credit cards.

The bank immediately fixed the configuration vulnerability that this individual exploited (a flaw in the firewall configuration for a web application) and promptly began working with federal law enforcement. The hacker suspected of being the author of the attack and arrested, is a former employee as a software engineer at a cloud computing company in Seattle. She published the data stolen on the GitHub coding platform; a user of the platform that saw the post informed Capital One of the data theft.

Capital One said it learned of the data breach on July 19 of this year and that the estimated cost of the security incident is between $ 100 million and $ 150 million in 2019, especially for customer notifications, credit monitoring and expenses for legal assistance.

The data breach compromised among others about 140,000 Social security numbers and 80,000 bank account numbers; the hacker was also able to access the personal information that customers (both private and small businesses) have released in their credit card application, such as phone number, physical address and e-mail address, risk assessment, the account balance. Fragments of transactions made during 2016, 2017 and 2018 were also compromised, not credit card numbers or log-in credentials, Capital One pointed out; 99% of the social security numbers in its database have not been touched.

Richard D. Fairbank, Chairman and CEO, apologized for the understandable incident and said that he will solve the problem, averting any impact on Capital One customers.

As some Kaspersky experts explained, the hacker exploited a weakness in the cloud platform configuration that the service provider used to store credit card data to steal data from the past 14 years. Furthermore, data can be used by hackers in different ways and can serve to falsify digital identities to facilitate fraud.

The massive scale of the leaked credit card applications could make this one of the biggest financial data breaches ever. The largest was the 2017 Equifax breach, in which the credit rating agency had suffered a computer intrusion to the detriment of 143 million people, almost exclusively US citizens. In recent days the group has agreed to pay a fine that could reach up to 700 million dollars and its title has not yet recovered the pre-cyber attack levels.

The main lesson to learn is that financial institutions need to manage cyber risk like they manage credit risk as part of their core competencies, so they must establish solid policies, controls, and test plans. The real challenge may be getting other types of businesses to do this.

Source: FORBES, Observations from the Fintech Snark Tank.

Link: https://www.forbes.com/sites/ronshevlin/2019/08/01/after-the-capital-one-data-breach/#8d4c4bc4ad19