One hack, 106 million people, Capital One ensnared by breach

30 July 2019, by Gene Johnson

In this July 16, 2019, file photo a Capital One credit card is shown in a wallet in San Francisco. A security breach at Capital One Financial, one of the nation's largest issuers of credit cards, compromised the personal information of about 106 million people, and in some cases the hacker obtained Social Security and bank account numbers. (AP Photo/Jeff Chiu, File)

A security breach at Capital One Financial, one of the nation's largest issuers of credit cards, compromised the personal information of about 106 million people, and in some cases the hacker obtained Social Security and bank account numbers.

It is among the largest security breaches of a major U.S. financial institution on record. The bank's stock tumbled 7% Tuesday, the largest single-day decline in four years.

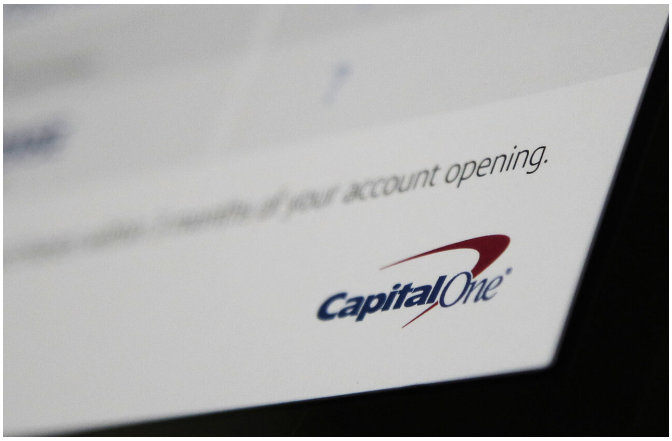
Paige A. Thompson, who uses the online handle "erratic"—was charged with a single count of computer fraud and abuse in U.S. District Court in Seattle. Thompson made an initial appearance in court and was ordered to remain in custody pending a detention hearing Thursday.

Federal agents began tracking Thompson online after being notified by Capital One of a possible breach in July.

On June 18, Thompson sent a message on Twitter to another user saying, "Ive basically strapped myself with a bomb vest, (expletive) dropping capitol ones dox and admitting it."

The FBI raided Thompson's residence Monday and seized digital devices. An initial search turned up files that referenced Capital One and "other entities that may have been targets of attempted or actual network intrusions."

Thompson was a systems engineer at Amazon Web Services between 2015 and 2016, about three years before the breach took place.



This Monday, July 22, 2019, photo shows Capital One mailing in North Andover, Mass. Capital One says a hacker got access to the personal information of over 100 million individuals applying for credit. The McLean, Virginia-based bank said Monday, July 29, 2019, it found out about the vulnerability in its system July 19 and immediately sought help from law enforcement to catch the perpetrator. (AP Photo/Elise Amendola)

In this July 16, 2019, file photo, a man walks across the street from a Capital One location in San Francisco. A security breach at Capital One Financial, one of the nation's largest issuers of credit cards, compromised the personal information of about 106 million people, and in some cases the hacker obtained Social Security and bank account numbers. (AP Photo/Jeff Chiu, File)

A resume Paige Thompson posted on a Slack group she created says she worked on its front-end the interface with users and security updates.

While that service is used by Capital One, there is no evidence that Amazon's cloud system was involved in the breach.

"AWS was not compromised in any way and functioned as designed," a company spokesperson said Tuesday. "The perpetrator gained access through a misconfiguration of the web application and not the underlying cloud-based infrastructure. As Capital One explained clearly in its disclosure, this type of vulnerability is not specific to the cloud."

Capital One Financial Corp. was notified by a third party on July 19 that their data had appeared on the code-hosting site GitHub, which is owned by Microsoft. The McLean, Virginia, company says it immediately notified the FBI.

The FBI said a Twitter user who went by "erratic" sent a user direct messages warning about distributing the bank's data, including names, birthdates and Social Security numbers. That user reported the message to Capital One.

This July 22, 2019, photo shows Capital One mail in North Andover, Mass. A security breach at Capital One Financial, one of the nation's largest issuers of credit cards, compromised the personal information of about 106 million people, and in some cases the hacker obtained Social Security and bank account numbers. It is among the largest security breaches of a major U.S. financial institution on record. The bank's stock dipped 6% at the opening of trading Tuesday, July 30. (AP Photo/Elise Amendola)

Capital One said it believes it is unlikely that the information was used for fraud, but the investigation is ongoing.

The data breach involves about 100 million people in the U.S. and 6 million in Canada.

The bank said the bulk of the hacked data consisted of information supplied by consumers and small businesses who applied for credit cards between 2005 and early 2019. In addition to data such as phone numbers, email addresses, dates of birth and self-reported income, the hacker was also able to access credit scores, credit limits and balances, as well as fragments of transaction information from a total of 23 days in 2016, 2017 and 2018.

"While I am grateful that the perpetrator has been caught, I am deeply sorry for what has happened," said Capital One CEO Richard Fairbank. "I

sincerely apologize for the understandable worry this incident must be causing those affected and I am committed to making it right."

Capital One Financial Corp., the nation's seventh-largest commercial bank with $373.6 billion in assets as of June 30, is the latest U.S. company to suffer a major data breach in recent years.

The logo for Capitol One Financial appears above a trading post on the floor of the New York Stock Exchange, Tuesday, July 30, 2019. A security breach at Capital One Financial, one of the nation's largest issuers of credit cards, compromised the personal information of about 106 million people, and in some cases the hacker obtained Social Security and bank account numbers. (AP Photo/Richard Drew)

In 2017, a data breach at Equifax, one of the major credit reporting companies, exposed the Social Security numbers and other sensitive information of roughly half of the U.S. population.

Last week, Equifax agreed to pay at least $700 million to settle lawsuits over the breach in a settlement with federal authorities and states. The agreement includes up to $425 million in monetary relief to consumers.

Many major banks have sought to stem the risk of data breaches in recent years. JPMorgan Chase, Bank of America and Citibank began replacing customers' debit cards several years ago with more secure chip-based cards. While the cards with chips are common these days, many merchants still rely on the older, less secure card-swiping equipment. Credit card companies have also beefed up fraud monitoring in the wake of high-profile data breaches that hit retailers such as Target and Home Depot.

The average cost of a data breach in the U.S. last year was just under $8 million, according to a study by IBM Security and Ponemon Institute.

A public defender appointed to represent Thompson did not immediately return an email seeking comment.

APA citation: One hack, 106 million people, Capital One ensnared by breach (2019, July 30) retrieved 21 October 2019 from https://techxplore.com/news/2019-07-capital-massive-breach.html