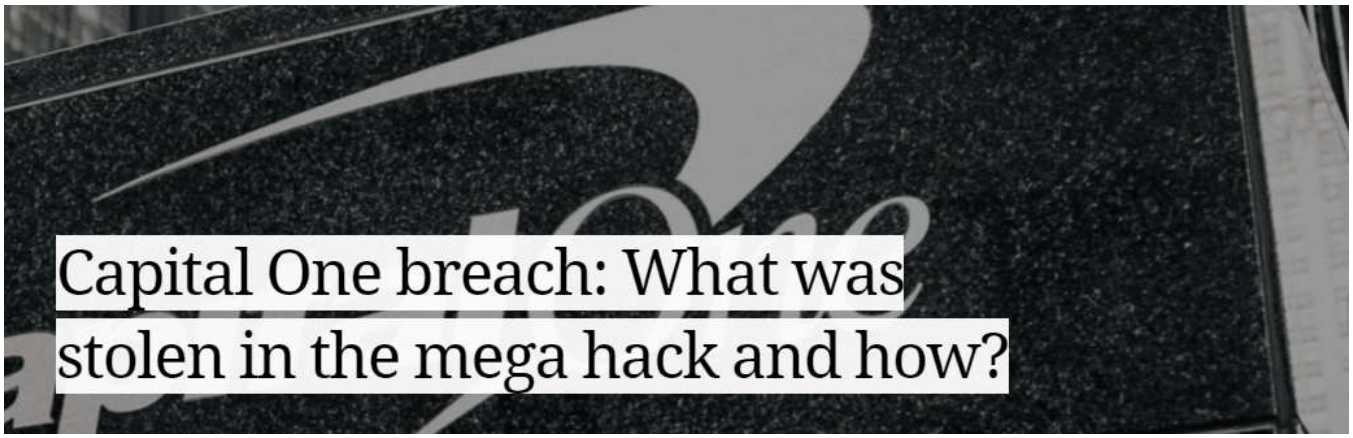
VERDICT



Written by Robert Scammell / Published on 22nd November 2018

Financial services firm Capital One has confirmed that it suffered a data breach in which some 106 million customer records were stolen by a hacker.

Stolen personal data included names, addresses, phone numbers, email addresses and dates of birth, as well as some financial details.

Approximately 100 million of the affected customers are in the US, with the remaining six million in Canada.

The Capital One breach was discovered on 19 July 2019. The hack took place on 22 and 23 March.

On Monday, the FBI arrested the person allegedly responsible: Paige Thompson, a 33-year-old former systems engineer at an undisclosed cloud computing firm. She is also believed to have worked for Amazon Web Services from May 2015 to September 2016.

Seattle court records show that she was charged with one count of computer fraud and abuse.

In a statement, Capital One chairman and CEO Richard D. Fairbank said:

"While I am grateful that the perpetrator has been caught, I am deeply sorry for what has happened. I sincerely apologise for the understandable worry this incident must be causing those affected and I am committed to making it right."

What else was stolen in the Capital One breach?

The most common type of data accessed related to information on consumers and small businesses.

In addition to the previously mentioned personal data, the hacker exfiltrated self-reported income, credit scores, payment history and "fragments of transaction data" from a total of 23 days, spread across a three-year period.

Somewhat misleadingly, Capital One said that "no bank account numbers or Social Security numbers were compromised". The financial firm then went on to state that "about 140,000 Social Security numbers of our credit card customers" and "about 80,000 linked bank account numbers of our secured credit card customers" had been compromised.

Capital One also said that the Social Insurance Numbers of approximately one million Canadian credit card customers were stolen in the breach.

Capital One breach: How did the hacker steal the data?

Court documents show that "a firewall misconfiguration permitted commands to reach" data buckets of data containing customer records. The hacker then executed these commands to exfiltrate the data.

“All it took was a misconfigured firewall and an experienced software engineer with some clever knowhow to compromise all of this data,” said Jake Moore, cybersecurity specialist at ESET.

“It is thought that the alleged criminal hacker once worked for Amazon Web Services, which makes this attack more of an insider threat and should remind companies how important it is to not overlook such risk.”

According to the court affidavit, Thompson used the alias “erratic” to talk about the Capital One data online. Another individual who saw Thompson’s online posts then notified Capital One that the stolen data appeared to be on code repository GitHub.

Sam Curry, chief security officer at Cybereason, said that Thompson’s alias was “aptly named” and that it appeared “that at least part of her motive was ego-driven and she has something to prove, implying that she may not have ties to organised crime or have sold this data”.

Although Capital One encrypts all its data, the bank said its data was decrypted during the breach.

“Due to complex key management and the fact that keys can be shared or exposed, classic encryption can fail,” said Felix Rosbach, product manager at Comforte AG, an enterprise data security provider.

He added that the reason comparatively few social security numbers and account numbers were stolen was because Capital One used tokenisation to protect this type of data. This sees sensitive data replaced with unique identification symbols that have no extrinsic value on their own.

“However, recent tokenisation technology could have been used to protect not only social security numbers and account numbers but also personal information, customer status data and transaction data,” added Rosbach.

“Castle and moat security isn’t effective anymore”

Capital One said it “immediately fixed the configuration vulnerability” used to gain access. It added that the vulnerability was not because it operated on the cloud.

However, Matt Walmsley, EMEA director at cybersecurity firm Vectra, said:

“Cloud services, with all their many benefits, also come with unique security risks to be managed such as attacks directly aimed at cloud PaaS using stolen credentials, which would remain invisible to workload and cloud instance-centric security controls. Pervasive visibility across the enterprise, agnostic of environment type, is fundamental to security success.”

As the details continue to emerge, there are still many questions that remain unanswered. Terence Jackson, CISO at cybersecurity company Thycotic, said he wanted to know whether the attacker had admin access and how the data was exfiltrated without triggering any alerts.

“This is yet another example of why castle and moat security isn’t effective anymore,” said Jackson. “The threats are already inside.”

The fallout

The Capital One breach ranks as one of the biggest suffered by a major financial institution.

“It should always be remembered that one of the main reasons we have the GDPR is to protect the digital economy and banks are at the very centre of that,” said Robert Wassall, a data protection expert and director of legal services at cybersecurity firm ThinkMarble. “In other words, this isn’t ‘just another’ large scale data breach, it’s a very significant data breach.”

The Capital One hack has already been compared to the Equifax breach, in which some 127 million of its customers had their

personal data stolen in a 2017 mega-breach. The credit rating agency was recently hit with a record $700m settlementby the Federal Trade Commission (FTC).

Javvad Malik, security awareness advocate at Knowbe4, said the Capital One data breach had "echoes of Equifax" in its scale.

But he added that internal investigations leading to an arrest within two weeks "represents a quick turnaround".

"While threat detection capabilities may have been lacking in the ability to pick up the breach, the company was paying attention to disclosed reports and had a quick and competent response capability to hand," he said.

Capital One said it expects "incremental costs of approximately $100m to $150m in 2019" relating to the data breach. This will mainly be legal support costs, credit monitoring, customer notifications and technology costs.

However, the overall cost of the breach will likely be far higher, in terms of potential fines and legal action, as well as reputational damage. Capital One's share price fell 4% in after-hours trading following the news to $93.

Not exactly like Equifax

Alex Heid, chief research officer at SecurityScorecard, a cyber risk rating company, said: "Compared to Equifax, this breach does not appear to have had anywhere near the same amount of impact."

The Equifax breach, deemed one of the worst in US history, involved a much larger amount of compromised social security numbers and banking details compared to the Capital One data breach. And where stolen Equifax data was also sold online, the Capital One breach data does not appear to have been sold or distributed.

"The rapid response from CapitalOne in this case is commendable, this incident indicates the organisation has an active bug bounty

program and works with information security researchers to mitigate issues as they are discovered," added Heid.

This is likely to play more favourably to investigators when compared to the four years taken by Marriott to discover it was the victim of a data breach.

However, ESET's Moore said that letting customers know about the breach sooner would have helped them "defend against any fraud should the data reach the dark web".

Because the Capital One data breach appears to have only affected Americans and Canadians, there will not be any legal enforcement from European regulators, where GDPR threatens fines of 4% of global turnover.

"However, coming so relatively soon after the Equifax breach, this incident may cause US regulators or politicians ('lawmakers') to conclude that existing enforcement options are not strong enough – or being used enough – to effectively ensure that key businesses put enough resources into data security," said Wassall.

"After all, this should never have happened."