# Q&A: What to know about the Capital One data breach

July 30 2019, by Ken Sweet, Frank Bajak And Michelle Chapman


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)

One of the country's biggest credit card issuers, Capital One Financial, is the latest big business to be hit by a data breach, disclosing that roughly 100 million people had some personal information stolen by a hacker.

The alleged hacker, Paige A. Thompson, obtained Social Security and bank account numbers in some instances, as well other information such as names, birthdates, credit scores and self-reported income, the bank said Monday. It said no credit card account numbers or log-in credentials were compromised.

Capital One Financial is just the latest business to suffer a data breach. Only last week Equifax, the credit reporting company, announced a $700 million settlement over its own 2017 data breach that impacted half of the U.S. population. Other companies that have had breaches include the hotel chain Marriott, retail giants Home Depot and Target.

WHAT HAPPENED?

Thompson, 33, who uses the online handle "erratic," allegedly obtained access to Capital One data stored on Amazon's cloud computing platform Amazon Web Services in March. She downloaded the data and stored it on her own servers, according to the complaint.

Thompson was a systems engineer at Amazon Web Services between 2015 and 2016, about three years before the breach took place. The breach went unnoticed by Amazon and Capital One.

Thompson used the anonymous web browser Tor and a Virtual Private Network in extracting the data—typical methods hackers use to try to mask infiltrations—but she later boasted about the hack on Twitter and a chat group on Slack, posting screenshots as evidence of her exploit.

It was only after Thompson began bragging about her feat in a private

group chat with other hackers that someone reached out to Capital One to let them know on July 17.

Once the informant told Capital One the company closed the vulnerability. The company verified its information had been stolen by July 19 and started tracking Thompson and working with the FBI. The FBI raided Thompson's residence on 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."

WHAT DID THOMPSON TAKE?

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

Prosecutors said a misconfigured Capital One firewall let Thompson access folders of data that Amazon Web Services was hosting for the bank. Thompson sent a command that returned a list of more than 700 folders and copied data from an unspecified number of them. Capital One 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. The hacker also was able to gain some access to fragments of transactional information from dates in 2016, 2017 and 2018.

The bank said it believes it is unlikely that the information obtained was used for fraud, but the investigation is ongoing.

Capital One says 140,000 individuals had their Social Security numbers accessed, and another 80,000 had their bank account information accessed.

## HOW DID CAPITAL ONE HANDLE THE BREACH?

Capital One says once it learned of the breach on July 17, it immediately closed the vulnerability, and it was able to figure out what Thompson accessed 36 hours later, on July 19. The company was able to build a profile on Thompson from their internal investigation, and handed that to the FBI, who arrested her 10 days later, the day the bank disclosed the breach.

By contrast, it took Equifax six weeks before it publicly disclose its security incident, which was similar in size.

## WHAT TO DO

Capital One said it will reach out to those affected using "a variety of channels."

That bank said it will make free credit monitoring and identity protection available to everyone affected. The company also said that consumers can visit www.capitalone.com/facts2019 for more information. In Canada, information can be found at www.capitalone.ca/facts2019 .

Consumers should also obtain copies of their credit reports at AnnualCreditReport.com. By federal law, consumers can receive a free copy of their credit report every 12 months from each of the three big agencies—Equifax, Experian and TransUnion.

Look over all of your listed accounts and loans to make sure that all of your personal information is correct and that you authorized the transaction. If you find something suspicious, contact the company that issued the account and the credit-rating agency.

You may also want to consider freezing your credit, which stops thieves from opening new credit cards or loans in your name. This can be done online. Consumers can freeze their credit for free because of a law that President Donald Trump signed last year. Before that, fees were typically $5 to $10 per rating agency.

You'll need to remember to temporarily unfreeze your credit if you apply for a new credit card or loan. Also keep in mind that a credit freeze won't protect you from thieves who file a fraudulent tax return in your name or make charges against an existing account.

You should also change your passwords regularly. CreditCards.com industry analyst Ted Rossman recommends using a password aggregator like LastPass that helps create strong, unique passwords for all of your logins.