

LILY HAY NEWMAN SECURITY 08.29.2019 02:48 PM

Everything We Know About the Capital One Hacking Case So Far

A new indictment against alleged Capital One hacker Paige Thompson includes a few fresh details about the case.



GETTY IMAGES

AT THE END of July, the FBI and Capital One disclosed that the bank had suffered a massive data breach just a few months before, exposing personal and financial data from more than 100 million customers. The FBI arrested former Amazon employee Paige Thompson, 33, in connection with the crime, and accused her of also breaching 30 other companies and organizations. Now, an indictment unsealed on Wednesday offers a fuller picture of the government's allegations against Thompson, and the scope of her alleged hacking spree.

Thompson, who also goes by the online handle "erratic," allegedly created a program in late March to scan cloud customers for a specific web application firewall misconfiguration. The indictment only refers to the platform as the "Cloud Computing Company," but an Amazon spokesperson confirmed to WIRED that it was Amazon Web Services. Thompson's prior role at the company didn't lend her any insider access in this case. Once the tool found its target misconfiguration, Thompson allegedly exploited it to extract privileged account credentials for victim databases and other web applications.

"Thompson is charged with wire fraud and computer fraud and abuse for the intrusion into data of Capital One and more than 30 other entities," the Department of Justice said in a statement late Wednesday. "Law enforcement has identified

many of the victims whose data was accessed and is working to notify them."

"Cryptojacking offers an immediate payout."

- JAKE WILLIAMS, RENDITION INFOSEC

Court documents say that once Thompson gained access to victims' cloud infrastructure using the stolen credentials, she then allegedly accessed and exfiltrated data. But the indictment also claims that in some cases she used this access to set up cryptocurrency mining operations using victims' cloud computing power—a practice known as cryptojacking.

"It's not really surprising at all that the hacker was cryptojacking," says Jake Williams, a former NSA analyst and founder of the security firm Rendition Infosec. "It's easy to assign hypothetical value to compromised data, but it takes work to turn that into spendable currency. Cryptojacking offers an immediate payout."

Investigators still have not publicly named other victims, but the indictment notes that one is a state agency, one is a public research university, and one is a telecom company based outside the United States. Not all the data Thompson allegedly stole contained personally identifying information. But in the case of Capital One, the breach exposed 106 million credit card applications which included names, addresses, phone numbers, and dates of birth, along with 140,000 Social Security numbers, 80,000 bank account numbers, and some credit scores and transaction data.

Thompson, who faces up to 25 years in prison, has been in police custody since her arrest on July 29. A transgender woman, she has been held in the SeaTac, Washington Federal Detention Center in a men's ward. Last week, a federal judge denied her request to be held with GPS monitoring in a halfway house. Based on her hacking skills and violent threats Thompson made online against herself and others, magistrate judge Michelle Peterson concluded that Thompson poses a physical and financial risk and may be a flight risk.

Thompson will be arraigned in Seattle District Court next week. The indictment doesn't speak to an alleged motive for the breaches, and it is unclear what happened to the stolen data once it was pilfered. Certainly millions of Capital One customers, and who knows how many as-yet unnamed victims, are hoping that the data didn't go far.



Case 2:19-cr-00159-RSL Document

1
2
3
4
5
6
7
8
9

Presented to the Court by the forer
Grand Jury in open Court, in the p
the Grand Jury and FILED in
DISTRICT COURT at Seattle, Wa

August 28
WILLIAM M. McCOI
By *[Signature]*

UNITED STATES DISTRI
WESTERN DISTRICT C
AT SEAT

More Great WIRED Stories

- Nobody's watching the best giant monster movies
- How to get the most out of your smartphone battery

- You're [racing toward a wall](#). Should you brake hard—or swerve
 - A history of plans to [nuke hurricanes](#) (and other stuff too)
 - For these [sword-wielding warriors](#), medieval battles live on
 - 👁 Facial recognition [is suddenly everywhere](#). Should you worry? Plus, read the [latest news on artificial intelligence](#)
 - 🛠 Optimize your home life with our Gear team's best picks, from [robot vacuums](#) to [affordable mattresses](#) to [smart speakers](#).
-



[Lily Hay Newman](#) is a senior writer at WIRED focused on information security, digital privacy, and hacking. She previously worked as a technology reporter at Slate magazine and was the staff writer for Future Tense, a publication and project of Slate, the New America Foundation, and Arizona State University. Additionally... [Read more](#)

SENIOR WRITER

TOPICS HACKING BREACHES
