Ex-Amazon Worker Convicted in Capital One Hacking

Paige Thompson's lawyers said she had been looking for cracks so they could be fixed. A jury found her guilty of wire fraud and hacking charges.

By Kate Conger
June 17, 2022

A former Amazon engineer who was accused of stealing customers' personal information from Capital One in one of the largest breaches in the United States was found guilty of wire fraud and hacking charges on Friday.

A Seattle jury found that Paige Thompson, 36, had violated an anti-hacking law known as the Computer Fraud and Abuse Act, which forbids access to a computer without authorization. The jury found her not guilty of identity theft and access device fraud.

Ms. Thompson had worked as a software engineer and ran an online community for other workers in her industry. In 2019, she downloaded personal information belonging to more than 100 million Capital One customers. Her legal team argued that she had used the same tools and methods as ethical hackers who hunt for software vulnerabilities and report them to companies so they can be fixed.

But the Justice Department said that Ms. Thompson had never planned to alert Capital One to the problems that gave her access to customers' data, and that she had bragged to her online friends about the vulnerabilities she uncovered and the information she downloaded. Ms. Thompson also used her access to Capital One's servers to mine cryptocurrency, the Justice Department said.

"She wanted data, she wanted money, and she wanted to brag," Andrew Friedman, an assistant U.S. attorney, said in closing arguments.

Ms. Thompson's case attracted attention from the tech industry because of the charges under the Computer Fraud and Abuse Act. Critics of the law have argued that it is too broad and allows for the prosecution of so-called white hat hackers. Last month, the Justice Department told prosecutors that they should no longer use the law to pursue hackers who engaged in "good-faith security research."

The jury deliberated for 10 hours before finding Ms. Thompson guilty of five counts of gaining unauthorized access to a protected computer and damaging a protected computer, in addition to the wire fraud charges. She is scheduled to be sentenced on Sept. 15.

A lawyer for Ms. Thompson declined to comment on the verdict.

Capital One discovered the breach in July 2019 after a woman who had spoken with Ms. Thompson about the data reported the problem to Capital One. Capital One passed the information to the Federal Bureau of Investigation, and Ms. Thompson was arrested soon after.

Regulators said Capital One lacked the security measures it needed to protect customers' information. In 2020, the bank agreed to pay $80 million to settle those claims. In December, it also agreed to pay $190 million to people whose data had been exposed in the breach.

"Ms. Thompson used her hacking skills to steal the personal information of more than 100 million people, and hijacked computer servers to mine cryptocurrency," said Nicholas W. Brown, the U.S. attorney for the Western District of Washington, in a statement. "Far from being an ethical hacker trying to help companies with their computer security, she exploited mistakes to steal valuable data and sought to enrich herself."