New York (CNN Business) In one of the biggest data breaches ever, a hacker gained access to more than 100 million Capital One customers' accounts and credit card applications earlier this year.

Paige Thompson is accused of breaking into a Capital One server and gaining access to 140,000 Social Security numbers, 1 million Canadian Social Insurance numbers and 80,000 bank account numbers, in addition to an undisclosed number of people's names, addresses, credit scores, credit limits, balances, and other information, according to the bank and the US Department of Justice. A criminal complaint says Thompson tried to share the information with others online. The 33-year-old, who lives in Seattle, had previously worked as a tech company software engineer for Amazon (AMZN) Web Services, the cloud hosting company that Capital One was using, the Justice Department said. She was able to gain access by

exploiting a misconfigured web application firewall, according to a court filing.
Thompson was arrested Monday in connection with the breach, the Justice Department said. Thompson's attorney could not be immediately reached for comment.

Capital One (COF) said the hack occurred March 22 and 23 and includes credit card applications as far back as 2005. The company indicated it fixed the vulnerability and said it is "unlikely that the information was used for fraud or disseminated by this individual." However, the company is still investigating.

"I sincerely apologize for the understandable worry this incident must be causing those affected and I am committed to making it right," said Capital One CEO Richard Fairbank in a statement.
The breach affected around 100 million people in the United States and about 6 million people in Canada, according to Capital One.

However, "no credit card account numbers or log-in credentials were compromised and over 99% of Social Security numbers were not compromised," the company noted.
Capital One said it will notify people affected by the breach and will make free credit monitoring and identity protection available. The company expects to incur between $100 million and $150 million in costs related to the hack,

including customer notifications, credit monitoring, tech costs and legal support due to the hack.
Capital One's stock was down 5% in premarket trading Tuesday.

How Capital One got hacked

The criminal complaint against Thompson paints a picture of a less-than-careful suspect.
Thompson posted the information on GitHub, using her full first, middle and last name, the complaint says. She also boasted on social media that she had Capital One information.

In a channel on Slack, a chat service often used by businesses as well as other groups, Thompson explained the method she used to break into Capital One, the Justice Department alleges. She claimed to use a special command to extract files in a Capital One directory stored on Amazon's servers.

"I wanna get it off my server that's why Im archiving all of it lol," Thompson allegedly posted on Slack. One person was alarmed by what Thompson found, writing that the information was "sketchy," adding, "don't go to jail plz."
Thompson made little effort to disguise her identity. She allegedly used the screen name "erratic" on Slack, which was the same handle she used on a Twitter account and a Meetup chatroom page.

The FBI special agent who investigated Thompson believes Thompson tweeted that she wanted to distribute Social Security numbers along with full names and dates of birth.

One person who saw the information on GitHub notified Capital One of the "leaked data" belonging to the company. Capital One notified the FBI, and an agent searched Thompson's residence on Monday. They found devices in her possession that reference Capital One and Amazon as well as other entities that may have been targets of attempted — or actual -- breaches.
The complaint indicates Thompson "recognizes that she has acted illegally."