Capital One hack compromises personal data of 106 million credit card applicants

By Kevin Reed
9 August 2019

Capital One Financial Corporation announced on July 29 that it had been hacked 10 days earlier "by an outside individual who obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers."

A company press release reported that the personal information—including 140,000 Social Security numbers and 80,000 bank account numbers—of as many as 106 million Capital One consumer and small business applicants between 2005 and 2019 had been compromised. It also reported that "approximately 1 million Social Insurance Numbers" of Canadian credit card customers had been hacked.

Simultaneously with the Capital One announcement, the FBI reported that it had arrested Paige A. Thompson, a 33-year-old Seattle-area woman who was a former cloud computing services engineer, and charged her with computer fraud and abuse in connection with the Capital One data breach, one of the largest to ever impact a financial institution.

According to the Capital One press release, the company immediately fixed "the configuration vulnerability" that had been exploited and added, "it is unlikely that the information was used for fraud or disseminated." It also said, "no credit card account numbers or log-in credentials had been compromised."

As with all such previous breaches of public personal information held by giant corporations, the number one priority of Capital One management is investor damage control and girding against the potential liability claims by the public. The stock of Capital One dropped by 6 percent on Wall Street the day after the revelations.

Under a subheading of "What are the expected financial impacts of the incident," the company does not focus upon the potential impact of the breach on consumer credit scores from the identity theft and fraud that will inevitably result from stolen social security numbers. Instead, Capital One reports that the breach will cost the company between $100 and $150 million from "consumer notifications, credit monitoring, technology costs and legal support."

The company further goes on in detail about how the losses will be reported on its financial results as well as the fact that Capital One has insurance that covers a "cyber-risk event," but it "is subject to a $10 million deductible and standard exclusions and carries a total coverage limit of $400 million." This is from a company that was worth $373.6 billion as of June 30 and had net earnings of $1.6 billion in the second quarter of 2019.

Capital One is a "bank holding company" headquartered in McLean, Virginia that specializes in various forms of consumer credit. It is the tenth largest bank in the US by assets, with offices in the US, Canada and the UK. Capital One created the mass marketing of credit cards in the 1990s and it is known for its annoying television commercials with various Hollywood celebrities who ask, "What's in your wallet?" The company was charged in 2012 with "misleading" customers into paying for services without asking and agreed to pay $210 million to provide refunds to 2 million card holders.

Several class action lawsuits have already been filed in connection with the recent data breach, saying that Capital One failed to take "reasonable care" to secure sensitive customer information. An attorney, John Yanchunis of Morgan and Morgan, representing in a case in Virginia, said, "You'd think with one data breach after another, companies would wise up and take responsibility for the data it collects from consumers, but unfortunately, they continue to shirk

that responsibility."

Subsequent reports on the technical aspects of the breach revealed that the hack was made possible by a misconfigured firewall in the cloud computing servers of Amazon Web Services. The *New York Times* reported that "Capital One was notified by a third party on July 17 that its data had appeared on the code-hosting site GitHub, which is owned by Microsoft."

The federal indictment filed against Paige A. Thompson on July 29 contains extensive computer forensic details about the breach and says that evidence links her to the intrusion in April and subsequent posting of Capital One information on the web hosting and project management site GitHub. The indictment says Thompson made statements on social media indicating "that she has information of Capital One, and that she recognizes that she has acted illegally."

FBI Special Agent and Cyber Squad Agent Joel Martini assembled the activity of Thompson on a variety of online services and put together a chronology of events from the first attempt to access the Capital One data on March 22 through July 17 when the company was notified of the breach by a third party. Specific details of Thompson's IP addresses, posts and communications on GitHub, IPredator (a prepaid VPN provider based in Sweden), Meetup, Slack and Twitter were gathered as part of the indictment.

Multiple news sources published profiles of Paige Thompson, who is a transgender woman, and depicted her as a brilliant engineer who struggled to find stability in her professional and personal life. She was the organizer of a Meetup Group called "Seattle Warez Kiddies" that was a forum for cyber topics including hacking.

Thompson's motivation for hacking the Capital One server as well as her apparent deliberate attempts to be "caught" for the crime are unclear. However, once the evidence was gathered by law enforcement, more than a dozen heavily armed agents in camouflage and helmets raided her residence, seized digital devices and arrested her.

The Capital One data breach is the latest in a long list of similar events in recent years where corporate entities entrusted with protecting critical consumer information are hacked relatively easily. Hundreds of millions of users and accounts have been hacked at LinkedIn, Yahoo, Target, eBay, Equifax and Marriott—to name a few of the largest—over the past decade.

The primary difference in this particular instance is that the hack was revealed simultaneously with the federal indictment and FBI arrest of the alleged hacker. Regardless of who is carrying out the hacks or the lackadaisical attitude of the entities responsible, the data breaches are being seized upon by the corporations as a pretext for increasingly invasive cyber-security measures and state attacks on democratic rights.