Yahoo-oops! At least 500M user accounts compromised

James J. Giszczak, Dominic A. Paluzzi | Friday, September 23, 2016

Yesterday, Yahoo confirmed that at least 500 million user accounts had information compromised in a massive cyber attack dating back to 2014 that it believes was perpetrated by a "state-sponsored actor." The scale of the breach makes it among the largest on record and serves as another stark reminder of why it's important for companies to have a comprehensive, proactive approach to data privacy and cybersecurity.

According to a statement released by Yahoo, "[t]he account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers." The company says its ongoing investigation into the hack suggests the stolen data does not include unprotected passwords, payment card data, or bank account information, which are all stored in a different system. The investigation has also found no evidence that the apparent state-sponsored actor is currently in Yahoo's networks, according to the company.

Following Yahoo's public announcement, Reuters reported that three U.S. intelligence officials, who declined to be identified, said they believed the attack was state-sponsored because of its resemblance to previous hacks traced to Russian intelligence agencies or hackers acting at their direction. Yahoo says it has been working closely with law enforcement on the breach. The FBI also issued a statement, saying that the agency "is aware of the intrusion…and will determine how it occurred and who is responsible," although it did not provide any information as to whether it had specific insight into who might have been behind the attack.

The disclosure of the massive data breach could not have come at a worse time for Yahoo. Just two months ago, Verizon announced plans to buy Yahoo's core properties for approximately $4.8 billion. A Verizon spokesperson confirmed that the company was notified of the incident "within the last two days," but has "limited information" on the attack and will evaluate as the investigation continues.

Although this may be the first time that the general public is learning about one of the largest data breaches in history, it is not necessarily the first time this hack is coming to light. Last month, a hacker named "Peace" claimed to have breached 200 million Yahoo usernames and passwords back in 2012, and offered to sell them on the dark web, after trying to do the same with MySpace and LinkedIn accounts. Yahoo's announcement on Thursday only cited the 2014 hack; it is unclear if the 2012 leak was related – but one can always speculate. The company did not respond to requests for clarification.

Yahoo will be contacting all potentially affected users by email. Users will be asked to change their passwords. Any unencrypted security questions and answers will be invalidated, meaning that users will have to submit new ones. Yahoo is also asking anyone who has not changed their password since 2014 to do so now for good measure. The company has also set up a frequently asked questions page for anyone who may have been affected by the breach.

In addition to the precautionary measures noted above, another critical step that all affected users should take is to identify any other online accounts they have

where they used the same username and/or password, and change the password to that account as well.

On the flip side, companies should always require strong passwords from users at the outset (i.e., during the registration phase) or, alternatively, shift from passwords to more reliable authentication options, such as multi-factor authentication. Most importantly, companies should provide notification to affected users as soon as possible following the discovery of a breach involving users' personally identifiable information.

To learn more about the types of protective measures companies can take to avoid situations like the one Yahoo experienced, please contact one of the data privacy and cybersecurity attorneys below.

James J. Giszczak

Dominic A. Paluzzi