Yahoo faces flurry of lawsuits hours after latest breach disclosure (N.D.Cal.)

(December 20, 2016) - Almost immediately after Yahoo Inc. made its second announcement in under three months that it had failed to stop another one of the largest data breaches ever disclosed, users again began pelting the technology giant with putative class actions.

Vail v. Yahoo Inc., No. 16-cv-7154, *complaint filed*, 2016 WL 7320954 (N.D. Cal. Dec. 14, 2016).

Baker v. Yahoo Inc., No. 16-cv-4601, *complaint filed*, 2016 WL 7335688 (N.D. Ga. Dec. 14, 2016).

Mortensen v. Yahoo Inc., No. 16-cv-7182, *complaint filed*, 2016 WL 7320857 (N.D. Cal. Dec. 15, 2016).

Gonzalez v. Yahoo Inc., No. 16-cv-7206, *complaint filed*, 2016 WL 7335685 (N.D. Cal. Dec. 16, 2016).

Yahoo announced Dec. 14 that an unauthorized party stole personal data likely associated with more than 1 billion accounts, a disclosure that came on the heels of the company's Sept. 22 announcement that it had discovered a separate massive hack.

Also on Dec. 14 New York resident Amy Vail filed a complaint in the U.S. District Court for the Northern District of California accusing Yahoo of providing inadequate security that left users' personal data vulnerable to hackers.

Vail's complaint cites a Dec. 14 blog post from Yahoo Chief Information Security Officer Bob Lord revealing that an as-yet unidentified party accessed user data in August 2013.

"For potentially affected accounts, the stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers," Lord wrote.

Vail's suit, one of a handful of potential class actions filed in California, accuses Yahoo of negligence, breaching the terms of its service agreement and privacy policy, and violating a California law aimed at unlawful and unfair business practices.

Craig A. Newman, New York-based head of Patterson Belknap Webb & Tyler's privacy and data security practice, said Vail's claims are "par for the course" after a major data breach but that "it will take months — if not longer — to begin sorting out the facts."

Yahoo has disclosed the two hacks while "in the midst of selling itself to Verizon. It's a complicated dynamic, to say the least," Newman, who is not involved in the case, wrote in an email.

Another breach, more suits

Yahoo user Andrew J. Mortensen filed a class action Dec. 15 in the Northern District of California making accusations similar to those in Vail's suit, plus common law causes of action such as unjust enrichment and bailment.

Mortensen alleges Yahoo implemented inadequate security measures in breach of its duties under the bailment, a term for giving possession of personal data or other property but never transferring ownership.

Tabitha Baker, an Atlanta resident who filed a class action in the U.S. District Court for the Northern District of Georgia, says she has used Yahoo's services since 1994, when the company was founded.

She accuses the company of negligence and violating her state's Fair Business Practices Act of 1975, Ga. Code Ann. § 10-1-390, as well as the federal Stored Communications Act, 18 U.S.C.A. § 2702.

"Identity thieves can also use the [stolen personal information] to harm the class members through embarrassment, blackmail, or harassment in person or online," her complaint says.

This is not the first set of lawsuits over Yahoo's allegedly inadequate security measures.

In September Yahoo was hit with multiple suits, including one filed in Illinois federal court by Christopher Havron and Katelyn Smith, after the company disclosed a 2014 "state-sponsored" hack of more than 500 million user accounts.

According to Lord's Dec. 14 blog post, Yahoo believes that incident is likely distinct from the newly uncovered hack.

Protect yourself

Kon Leong, CEO and founder of ZL Technologies, said companies should take steps to protect themselves from similar breaches.

"Apart from best practices for password security, such as frequently prompting users to change passwords and never storing raw password data, there are a few things companies with user data should consider," Leong said. "For instance, client-side encryption is helpful to prevent raw passwords from being sent over the wire."

At the time of the breach, Yahoo was protecting passwords with MD5, a cryptographic hash function that changes a variable message into a sequence of 32 hexadecimal digits and which can be vulnerable to attacks, he said. Leong noted that the company has since moved on from the practice.

He also suggested that companies "make use of 'white hats,' guns for hire who will attempt to hack into a company's system as a way of detecting vulnerabilities."

Leong said Yahoo's users find themselves in a strange situation since the breach occurred so long ago and only limited facts about the intruder's intent are available. But they should still take steps now to secure their accounts, he said.

"Though it's likely any damage would have already been done by now, the first thing anyone with an account should do is to change their password and, often overlooked: their security questions and answers," Leong said.

"Users should also remove any sensitive information from their accounts so that in the event they are accessed, users can still retain anonymity," he added.

By Melissa J. Sachs

Related Articles

Related Articles from WESTLAW Data Privacy Daily Briefing
Article: Yahoo hid 'state-sponsored' data breach, suit says 2016 DPDBRF 0076
Date: Sept. 26, 2016
Two Illinois residents have sued Yahoo Inc. in federal court for breach of implied contract and unlawful business practices involving the recently disclosed "state-sponsored" hack of more than 500 million user accounts that occurred in 2014.

End of Document