THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit http://www.djreprints.com.

http://www.wsj.com/articles/hackers-post-stolen-user-data-from-ashley-madison-breach-1440032355

TECH

Hackers Post Stolen User Data From Ashley Madison Breach

Troves of company files apparently were placed onto 'dark Web'

Avid Life Media, the company that runs the site, was hacked last month. *PHOTO: ASHLEYMADISON.COM*

By **DANNY YADRON**

Updated Aug. 19, 2015 10:51 p.m. ET

Avid Life Media Inc. called a hacker's bluff—and lost.

In July, digital intruders claimed to have stolen user data for AshleyMadison.com, Avid Life's popular website that facilitates extramarital affairs. The hackers threatened to release the data unless Avid Life—then talking of a $200 million public stock offering—closed the service.

On Wednesday, Avid Life confirmed that some of the customer data posted this week in a dark corner of the Internet is legitimate. The disclosure sparked a frenzy as people tried to search for their own names and those of partners, while divorce lawyers said

they were searching for potential evidence and a British florist offered a discount on "apology flowers."

Avid Life's decision to face down the hackers raises tough moral and legal questions.

The demand was even more dramatic than that faced by Sony Pictures Entertainment late last year. Then, hackers believed to be affiliated with North Korea wanted the studio to cancel the release of a movie. Avid Life faced a request to close its best-known business, which claimed 38 million users.

Federal investigators often warn hacking victims not to comply with hackers' demands —fearing that will only embolden future attackers.

One problem of dealing with hackers is "you're putting your trust in someone who is inherently untrustworthy," said Andre McGregor, a former special agent with the Federal Bureau of Investigation and now the director of security at Tanium Inc., a San Francisco Bay Area cybersecurity company.

Lisa Sotto, a partner at Hunton & Williams LLP who specializes in data breaches, said Avid Life was put in an impossible position by the demand it shut down. But Ms. Sotto said the company could have done more in the past month to reach out to users who may have been affected. For instance, she said she noticed that AshleyMadison.com's home page on Wednesday still made no mention of the breach. Rather, users have to scroll through recent news releases in the press section of the site.

NBC News reported that Avid spokesman Paul Keable said at least some of the data posted online this week is legitimate. Mr. Keable and his associates didn't respond to phone calls and emails from The Wall Street Journal. An outside spokeswoman for Avid, Jennifer Tong, said only, "I don't have anything additional."

The hackers, or hacker, apparently dumped troves of company files onto the "dark Web," areas of the Internet not accessible by consumer browsers. The data included credit-card transactions and account details but not credit-card numbers, according to security researchers. In a statement on the Ashley Madison website, Avid said, "No current or past members' full credit card numbers were stolen."

It can be difficult to verify the true identities of Ashley Madison users. The company apparently didn't verify the email addresses that users supplied.

The website hosting the newly disclosed files can only be accessed through the Tor

browser, special software that allows for private Web surfing. That also means Avid Life will have a hard time getting the content taken offline.

As of Wednesday afternoon it was still posted, some 24 hours after it was first noticed by Wired magazine.

Dave

RELATED ARTICLES

- How Hackers May Have Hurt a Possible Ashley Madison IPO (http://blogs.wsj.com/moneybeat/2015/07/20/can-ashley-madison-still-go-public-post-hacking/)
- Hackers Target Users of Infidelity Website Ashley Madison (http://www.wsj.com/articles/affair-website-ashley-madison-hacked-1437402152)

Kennedy, chief executive at security firm TrustedSec, combed through the files posted online and found documents that he said seemed legitimate on Avid Life's computer systems and organizational structure. "The biggest indicators to legitimacy comes from these internal documents, much containing sensitive internal data," he wrote in a blog post.

Toronto-based Avid Life confirmed in July that its systems were breached and that hackers threatened to release data, including account holders' names, addresses and special Ashley Madison codes for their preferences. Avid Life said last month it forced file-sharing websites to take down samples of the stolen data initially published after the hack.

Brian Krebs, a security blogger, said several users verified their information was released and that the data appears real. But he earlier spoke to the founding chief technology officer for Ashley Madison, now a consultant with Avid Life, who said the company has seen many fake data dumps in the past month and that it wasn't certain this latest one was genuine.

Avid Life Media has carved out a niche in offering more thematic outlets for online dating. In addition to Ashley Madison, there's CougarLife.com aimed at older women seeking younger men. There's also EstablishedMen.com, which seeks to match rich businessmen with young women.

Along with the data apparently released Tuesday was a message titled "Time's Up" from Impact Team, the name used by the people or person behind the July breach. It repeats the team's earlier claims that Avid Life's websites are filled with fraudulent profiles, and that it charges members an excessive fee to wipe their information from the site.

"We have explained the fraud, deceit, and stupidity of ALM and their members," the post reads. "Now everyone gets to see their data."

On Wednesday evening, a spokesman for Avid Life referred questions about the breach to Cycura, a Toronto cybersecurity firm Avid Life hired to investigate the breach.

The Federal Bureau of Investigation and Royal Canadian Mounted Police are involved in the investigation, said a spokesman for Cycura.

—Orr Hirschauge contributed to this article.

Write to Danny Yadron at danny.yadron@wsj.com

Copyright 2014 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.