

Uber Scumbags Concealed Cyberattack That Exposed 57 Million People's Data

By Eric Newcomer

Company paid hackers \$100,000 to delete info, keep quiet

Chief Security Officer Joe Sullivan and another exec ousted

Hackers stole the personal data of 57 million customers and drivers from [Uber Technologies Inc.](#), a massive breach that the company concealed for more than a year. This week, the ride-hailing company ousted Joe Sullivan, chief security officer, and one of his deputies for their roles in keeping the hack under wraps.

Compromised data from the October 2016 attack included names, email addresses and phone numbers of 50 million Uber riders around the world, the company told Bloomberg on Tuesday. The personal information of about 7 million drivers were accessed as well, including some 600,000 U.S. driver's license numbers. No Social Security numbers, credit card details, trip location info or other data were taken, Uber said.

At the time of the incident, Uber was negotiating with U.S. regulators investigating separate claims of privacy violations. Uber now says it had a legal obligation to report the hack to regulators and to drivers whose

license numbers were taken. Instead, the company paid hackers \$100,000 to delete the data and keep the breach quiet. Uber said it believes the information was never used but declined to disclose the identities of the attackers.

“None of this should have happened, and I will not make excuses for it,” Dara Khosrowshahi, who took over as chief executive officer in September, said in an emailed statement. “We are changing the way we do business.”

Hackers have successfully infiltrated numerous companies in recent years. The Uber breach, while large, is dwarfed by those at Yahoo, MySpace, Target Corp., [Anthem Inc.](#) and [Equifax Inc.](#) What’s more alarming are the extreme measures Uber took to hide the attack. The breach is the latest explosive scandal Khosrowshahi inherits from his predecessor, [Travis Kalanick](#).

Kalanick, Uber’s co-founder and former CEO, learned of the hack in November 2016, a month after it took place, the company said. Uber had just settled a lawsuit with the New York attorney general over data security disclosures and was in the process of negotiating with the [Federal Trade Commission](#) over the handling of consumer data. Kalanick declined to comment on the hack.

Sullivan spearheaded the response to the hack last year, a spokesman told Bloomberg. Sullivan, a onetime federal prosecutor who joined Uber in 2015 from [Facebook Inc.](#), has been at the center of much of the decision-making that has [come back to bite Uber](#) this year. Bloomberg reported last month that the board commissioned an investigation into the activities of Sullivan’s security team. This project, conducted by an

outside law firm, discovered the hack and the failure to disclose, Uber said.

Here's how the hack went down: Two attackers accessed a private GitHub coding site used by Uber software engineers and then used login credentials they obtained there to access data stored on an Amazon Web Services account that handled computing tasks for the company. From there, the hackers discovered an archive of rider and driver information. Later, they emailed Uber asking for money, according to the company.

A patchwork of state and federal laws require companies to alert people and government agencies when sensitive data breaches occur. Uber said it was obligated to report the hack of driver's license information and failed to do so.

“At the time of the incident, we took immediate steps to secure the data and shut down further unauthorized access by the individuals,” Khosrowshahi said. “We also implemented security measures to restrict access to and strengthen controls on our cloud-based storage accounts.”

Uber has earned a reputation for flouting regulations in areas where it has operated since its founding in 2009. The U.S. has opened at least five criminal probes into possible bribes, illicit software, questionable pricing schemes and theft of a competitor's intellectual property, people familiar with the matters have said. The San Francisco-based company also faces dozens of civil suits. London and other governments have taken steps toward banning the service, citing what they say is reckless behavior by Uber.

In January 2016, the New York attorney general fined Uber \$20,000 for failing to promptly disclose an earlier data breach in 2014. After last year's cyberattack, the company was negotiating with the FTC on a privacy settlement even as it haggled with the hackers on containing the breach, Uber said. The company finally agreed to the FTC settlement three months ago, without admitting wrongdoing and before telling the agency about last year's attack.

The new CEO said his goal is to change Uber's ways. Uber said it informed New York's attorney general and the FTC about the October 2016 hack for the first time on Tuesday. Khosrowshahi asked for the resignation of Sullivan and fired Craig Clark, a senior lawyer who reported to Sullivan. The men didn't immediately respond to requests for comment.

The company said its investigation found that Salle Yoo, the outgoing chief legal officer who has been scrutinized for her responses to other matters, hadn't been told about the incident. Her replacement, Tony West, will start at Uber on Wednesday and has been briefed on the cyberattack.

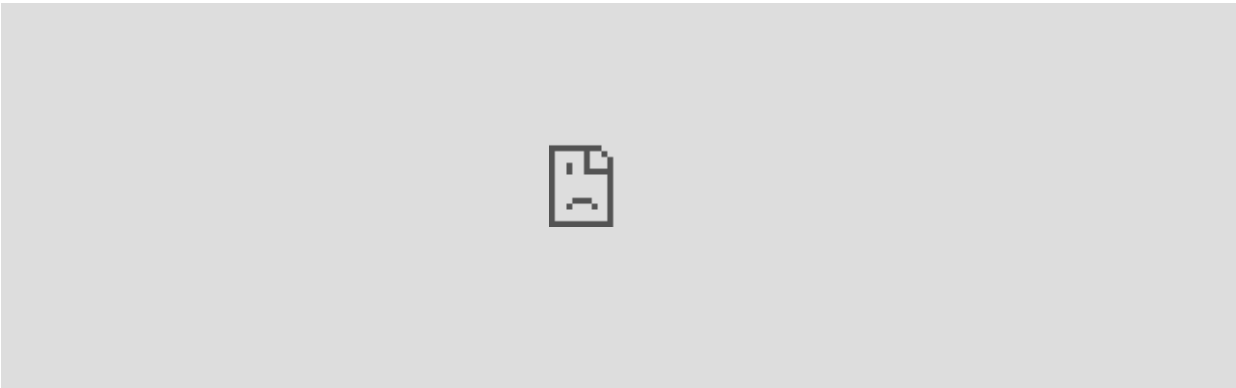
Kalanick was ousted as CEO in June under pressure from investors, who said he put the company at legal risk. He remains on the board and recently filled two seats he controlled.

"While I can't erase the past, I can commit on behalf of every Uber employee that we will learn from our mistakes," Khosrowshahi said in the emailed statement.

Uber said it has hired Matt Olsen, a former general counsel at the National Security Agency and director of the National Counterterrorism Center, as an adviser. He will help the company restructure its security teams. Uber hired Mandiant, a cybersecurity firm owned by [FireEye Inc.](#), to investigate the hack.

The company plans to release a [statement](#) to customers saying it has seen “no evidence of fraud or misuse tied to the incident.” Uber said it will provide drivers whose licenses were compromised with free credit protection monitoring and identity theft protection.

For more on Uber, check out the Decrypted podcast:



Before it's here, it's on the Bloomberg Terminal.

[LEARN MORE](#)

*Have a confidential news tip?
Get in touch with our reporters.*