6-BankInfoSecurity-Ubers British

Uber’s British Breach Tally: 2.7 Million Victims

Privacy Watchdog Warns Victims to Beware of Social Engineering Attacks
Mathew J. Schwartz (euroinfosec) • November 29, 2017

Credit Eligible

Get Permission

Beleaguered ride-sharing service Uber has informed Britain’s privacy regulator that 2.7 million riders and drivers had personal details exposed by a massive breach in 2016 that it covered up for a year *[Deny]*(see Uber Concealed Breach of 57 Million Accounts for a Year).

“Uber has said the breach involved names, mobile phone numbers and email addresses,” James Dipple-Johnstone, the deputy commissioner for the U.K. Information Commissioner’s Office - the country’s privacy watchdog - says in a statement.

Worldwide, the breach affected 57 million accounts used by Uber riders and drivers.

Dipple-Johnstone warned victims to beware of follow-on social engineering attacks.

“On its own, this information is unlikely to pose a direct threat to citizens. However, its use may make other scams, such as bogus emails or calls, appear more credible. People should continue to be vigilant and follow the advice from the NCSC,” he said, referring to the country’s National Cyber Security Center, *[Worry]*which includes the U.K. computer emergency response team (see Driving Privacy Regulators Crazy: UK Probes Uber Breach).

The ICO says its investigation into the breach is ongoing and that it is working with the U.S. Federal Trade Commission and other agencies. “As part of our investigation, we are still waiting for technical reports, which should give full confirmation of the figures and the type of personal data that has been compromised,” Dipple-Johnstone said. “We would expect Uber to alert all those affected in the UK as soon as possible.” *[Hope]*

The ICO can impose fines of up to £500,000 on organizations that violate the country’s privacy rules or mishandle people’s personal data. Under the EU General Data Protection Regulation, or GDPR, which will be enforced starting in May 2018, EU privacy watchdogs will gain the ability to impose fines of up to 4 percent of a company’s global annual profits, or €20 million ($23.5 million) - whichever is greater.

Hush Money?

Uber reportedly paid $100,000 to the two hackers who found the flaw and used it to exfiltrate data. *[Compliance]*

Uber has attempted to portray its $100,000 payment to the two hackers not as an extortion payoff but rather a “bug bounty,” despite the company’s official bug bounty program capping out at $10,000 (see Fast and Furious Data Breach Scandal Overtakes Uber).

New Uber CEO Dara Khosrowshahi, who started his job less than three months ago, said he didn’t learn about the breach until nearly a month into his tenure. *[Deny]* He then waited two months, pending the results of an investigation, to issue a public notification about the breach (see Did Uber Break Breach Notification Minimum-Speed Limits?).

Khosrowshahi said that in the meantime, he was cleaning house. The company fired CSO Joe Sullivan and his deputy, Craig Clark, for what it said was their poor handling of the breach *[Deny]*. Neither Sullivan nor Clark, however, have spoken about the circumstances leading to their departure. Their side of the story could emerge if Congress asks them to testify about the breach.

Legal Woes

The breach adds to Uber’s mounting woes as it’s struggling to finalize a $10 billion investment from a consortium led by SoftBank Group. At the same time, a string of senior executives have recently departed the business, and Uber also lost its license to operate in London earlier this year.

The company faces a number of probes and lawsuits over alleged sexism and harassment as well as working conditions and the alleged theft of self-driving car trade secrets from Google parent Alphabet’s Waymo unit, which Uber denies.

But on Tuesday, U.S. District Judge William Alsup of San Francisco delayed a trial in the case involving Alphabet and Uber after a letter written by a former member of Uber’s security team, Ric Jacobs, was read aloud in court. The letter alleged that Uber had created a team designed to steal competitors’ trade secrets, and that it used devices and services designed to store information away from Uber’s official systems to help evade regulatory scrutiny, the Wall Street Journal reported.

“We’re going to have to put the trial off because if even half of what’s in that letter is true it would be a huge injustice to force Waymo to go to trial,” Judge Alsup said at the Tuesday hearing, the Wall Street Journal reports.