Uber breach could affect the data of 50K drivers

The ride-hailing service says it was the victim of a hack last May that could have exposed thousands of driver names and driver's license numbers.

February 27, 2015 By: Dara Kerr CNET Magazine

http://www.cnet.com/news/uber-breach-could-affect-the-data-of-50k-drivers/

Uber announced Friday that one of its databases was possibly breached last year, which could have put up to 50,000 former and current Uber drivers' personal information at risk.

The breach was first discovered on September 17 of last year and Uber believes it was a onetime incident that happened on May 13, 2014. The database held the names and driver's license numbers of thousands of Uber drivers in multiple states. Uber is a ride-hailing service that lets passengers connect with drivers via a smartphone app.

Though the private information of 50,000 people is a lot, it's small compared with the dozens of hacks on other companies over the past couple of years. Retailers and banks, like Target, Home Depot and **JPMorgan**, **experienced massive security breaches** in 2013 and 2014. In the case of Target, **110 million people's personal information** was exposed; and in the Home Depot hack **56 million credit cards**were put at risk.

Uber said the security breach was perpetrated by an "unauthorized third party" but didn't say how it discovered the vulnerability.

As soon as Uber found out about the breach it changed access to the database to stop any further leaks, the company said. It's now notifying the drivers whose information was in the database and is offering them a free year membership to credit-monitoring company Experian.

"We have not received any reports of actual misuse of information as a result of this incident," Uber's managing counsel of data privacy, Katherine Tassi, said in a **statement**.

Security breaches have become so pervasive over the last year that earlier this month President Barack Obama signed an executive order addressing the issue. The order is meant to**establish a framework** to help businesses and government organizations "prioritize and optimize" their spending and quickly identify and protect themselves against cyberattacks.