

September 28, 2018

Steve Marshall
Alabama Attorney General



For More Information, contact:

Mike Lewis (334) 353-2199

Joy Patterson (334) 242-7491

Page 1 of 2

AG Steve Marshall Announces Settlement with Uber to Enforce and Strengthen Data Breach Protections

(MONTGOMERY)—Attorney General Steve Marshall announced Alabama has participated in a nationwide settlement with Uber that compels the company to comply with data breach notification laws and to make substantial improvements to its data security measures. In addition, Uber will pay a total of \$148 million to the states, with the State of Alabama receiving \$2 million.

All 50 states and the District of Columbia joined the settlement with the California-based ride-sharing company, Uber Technologies Inc., to resolve issues arising from a 2016 data breach involving personal information of Uber drivers that the company failed to report for one year.

Because Alabama did not have a data breach notification law in effect at the time of the violations, the State's participation in this case was based upon the fact that Uber's conduct violated Alabama's Deceptive Trade Practices Act.

"This situation underscores how important Alabama's new data breach notification law is for our consumers," said Attorney General Marshall. "People have the right to know if their personal information is stolen or compromised in a data breach so that they may exercise vigilance and take any actions possible to protect themselves. Until this year, Alabama was one of only two states without a data breach notification law, and I am pleased we were successful in passing legislation to correct that omission."

Uber learned in November 2016 that hackers had gained access to some personal information that Uber maintains about its drivers, including driver's license information pertaining to approximately 600,000 drivers nationwide. Uber tracked down the hackers and obtained assurances that the hackers deleted the information even though some of that information, namely the driver's license numbers for Uber drivers, triggered many state laws requiring them to notify those affected, Uber failed to report the breach in a timely manner, waiting until November 2017 to report it.



In addition to the financial payment to the states, the settlement requires Uber to strengthen its corporate governance and data security practices to help prevent a similar occurrence in the future.

The settlement requires Uber to:

- Comply with all state data breach and consumer protection laws regarding the protection of consumers' personal information and notifying them in the event of a data breach concerning that information;
- Take precautions to protect any user data Uber stores on third-party platforms outside of Uber;
- Use strong password policies for its employees to gain access to the Uber network;
- Develop and implement a strong overall data security policy for all data that Uber collects about its users, including assessing potential risks to the security of the data and implementing any additional security measures beyond what Uber is doing to protect the data;
- Hire an outside qualified party to assess Uber's data security efforts on a regular basis and draft a report with any recommended security improvements, which Uber will then implement; and
- Develop and implement a corporate integrity program to ensure that Uber employees can bring any ethics concerns they have about any other Uber employees to the company, and that it will be heard.

Attorney General Marshall commended the staff of his Consumer Interest Division for their work in bringing this case to a successful conclusion.