



NEWS RELEASE

Marty J. Jackley
South Dakota Attorney General

Charles McGuigan
Chief Deputy Attorney General

FOR IMMEDIATE RELEASE: Wednesday, September 26, 2018
CONTACT: Sara Rabern (605) 773-3215

Attorney General Jackley Reaches Settlement Agreement with Uber over Data Breach

PIERRE, S.D. – Attorney General Marty Jackley announced today that he, along with the other 49 states and the District of Columbia, has reached an agreement with ride-sharing company Uber Technologies, Inc. (Uber) to address the company’s one-year delay in reporting a data breach to its affected drivers.

Uber learned in November 2016 that hackers had gained access to some personal information that Uber maintains about its drivers, including drivers’ license information pertaining to approximately 600,000 drivers nationwide. Uber tracked down the hackers and obtained assurances that the hackers deleted the information. However, Uber failed to report the breach in a timely manner, waiting until November 2017 to report it.

“Reporting a data breach allows consumers to minimize the risk of harm done to their personal identifying information and law enforcement to better protect consumers,” said Jackley. “Nationwide data breaches will continue to occur, and failure to timely report the loss of sensitive information further harms victims of the breach.”

As part of the nationwide settlement, Uber has agreed to pay \$148 million to the states. South Dakota will receive \$573,488.83. In addition, Uber has agreed to strengthen its corporate governance and data security practices to help prevent a similar occurrence in the future.

The settlement between the state of South Dakota and Uber requires the company to:

- Comply with South Dakota data breach and consumer protection law regarding protecting residents’ personal information and notifying them in the event of a data breach concerning their personal 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. Uber will implement any such security improvement recommendations; 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.