ROPES & GRAY

ALERT ▪ Privacy & Cybersecurity

October 12, 2018

Fifty State Attorneys General Reach Settlement over Cyber-Incident Disclosure

Attorneys
Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Seth C. Harrington
Mark P. Szpak
Michelle Visser
David T. Cohen
Rebecca Harlow

Uber Technologies, Inc. has reached a settlement with the attorneys general for all fifty states and the District of Columbia regarding allegations that Uber had violated state data breach notification statutes and consumer protection laws in connection with a 2016 data breach.

The monetary settlement is the largest state attorneys general settlement reached in the aftermath of a data breach and the first to include every state in the nation. It is also the most recent step in a trend of state law enforcement becoming increasingly aggressive in pursuing companies that have suffered data breaches, especially with regard to disclosure requirements.

The state attorneys general asserted consumer protection claims relating to Uber’s data security practices and also asserted that the allegedly delayed announcement violated state statutes regarding notification of data breaches within specific periods of time or within a “reasonable” time or as prompt as is practicable.

For instance, many states, including California and New York, require that “disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.” Maryland adds the requirement that the reasonably expedient disclosure occur within 45 days of the completion of an investigation into an incident. New Mexico and several other states cap the reporting period at 45 days from the discovery or confirmation of a breach.

Uber publicly disclosed the unauthorized access to data about users and drivers, including as many as 57 million individuals worldwide (with 25.6 million in the United States), in November 2017, approximately a year after the incident occurred.

The Uber settlement is significantly larger than others reached with state attorneys general in recent years. For example, in 2017, multistate groups of attorneys general announced two settlements following data security incidents that had occurred previously. Nationwide paid $5.5 million to a group of 32 states and the District of Columbia in connection with a 2012 incident that allegedly may have involved the data of 1.27 million people. Target agreed to pay $18.5 million to settle claims arising out of its 2013 incident that allegedly involved approximately 40 million payment cards and the personal information of as many as 70 million individuals. At the time, the Target settlement was the largest of its kind.

In addition to paying $148 million to be divided among the states, Uber has committed to certain business practices, including specific data protection steps, password standards, encryption, development of an information security plan and an incident response and breach notification plan, and ongoing self-assessment of data security.

For more information regarding the Uber settlement, or to discuss cybersecurity practices generally, please feel free to contact Heather Sussman, Doug Meal, Jim DeGraw, Seth Harrington, Mark Szpak, Michelle Visser, David Cohen, Rebecca Harlow, or another member of Ropes & Gray’s leading privacy & cybersecurity team.

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have.