CLIENT ALERT

Uber Reaches $148 Million Data Breach Settlement With State Attorneys General

September 28, 2018

AUTHORS

Elizabeth J. Bower | James C. Dugan | Daniel K. Alvarez | Philip F. DiSanto

On September 26, 2018, Uber Technologies, Inc. ("Uber"), a prominent ride-sharing technology and transportation company, reached a $148 million nationwide settlement with the attorneys general of all 50 states and the District of Columbia (the "AGs") to resolve claims that it violated state laws protecting consumers and personal information (the "Settlement"). The Settlement took the form of a Final Judgment and Consent Decree that provides for both a record-breaking financial penalty and significant ongoing compliance obligations.

The Settlement is consistent with a recent wave of state investigations, enforcement actions, and legislative reforms focused on the protection of personal information and the timely reporting of any incidents. In announcing the Settlement, the AGs emphasized that Uber's lack of transparency and failure to promptly report the breach justified a particularly robust response. The Settlement provides guidance for companies in charting their own paths through the current cyber risk environment.

Background

In November 2017, Uber disclosed that it had suffered a data breach that compromised the personal information of up to 57 million individuals. According to the AGs' complaint, Uber first became aware of the breach during the prior year when it was approached by hackers who demanded payment in exchange for deleting data that had allegedly been accessed and acquired from Uber. Uber identified the vulnerability, paid the hackers to delete the data (and verify deletion), and proceeded as if that vulnerability had been identified through its "bug bounty" program. However, Uber did not disclose the breach to the public, government authorities, or the individuals whose personal information was compromised.

Immediately following the announcement, Uber faced investigations by the AGs and the Federal Trade Commission, along with numerous private consumer class-action lawsuits.

Assessment of Record Financial Penalty

Uber agreed to pay a record-breaking financial penalty of $148 million to settle the AGs' investigations and claims. The payment will be divided between all 50 states and the District of Columbia and will presumably be used, in part, to fund future data security enforcement efforts by state and local authorities.

Decade-Long Compliance Requirements

In addition to the massive financial penalty, however, the Settlement also requires that Uber implement the following privacy and data security practices:

1. **Specific Data Security Safeguards**: Uber must implement and maintain for 10 years specific data security safeguards that include (i) restrictions on cloud-based services and platforms from third parties, (ii) strong employee password requirements, and (iii) encryption of personal information of Uber riders and drivers.

2. **Information Security Program**: Uber must develop, implement, and maintain a comprehensive information security program that accounts for (i) "the size and complexity of UBER's operations," (ii) "the nature and scope of UBER's activities," and (iii) "the sensitivity of the Personal Information of Riders and Drivers that UBER maintains." Uber's comprehensive security program must include, among other things, the implementation and testing of reasonable safeguards that address internal and external risks, ongoing employee and contractor training, and the designation of an executive or officer with "appropriate background and experience in information security" to oversee the security program.

3. **Information Security Program Assessments**: Uber must obtain biennial assessments for 10 years of its information security program from an independent third party that is qualified to conduct such assessments. Each assessment must be memorialized in a final written report that is to be provided to the California Attorney General's Office within 120 days of the assessment's completion.

4. **Incident Response and Data Breach Notification Plan**: Uber must report to the Iowa Attorney General on a quarterly basis any data security incident that must be reported to any U.S. federal, state, or local government entity, pursuant to "any U.S. federal, state, or local law or regulation . . . ." In addition, Uber must maintain a comprehensive incident response and data breach notification plan that requires, among other things, (i) clear descriptions of individuals' roles and responsibilities, (ii) regular testing of the plan, (iii) active involvement of attorneys in assessing notification obligations, and (iv) quarterly reports to Uber's Chief Executive Officer, Chief Legal Officer, and Board of Directors on the number of data security incidents and how they were resolved.

5. **Corporate Integrity Program**: Uber must also adopt a corporate integrity program to address perceived issues with Uber's corporate culture. The corporate integrity program must mandate that Uber's designated security executive "advise the Chief Executive Officer or the Chief Legal Officer of UBER's security posture, security risks faced by UBER, and security implications of UBER's business decisions."

The Settlement builds on recent efforts by state AGs to impose stringent privacy and data security compliance obligations on companies that suffer data breaches. In May 2017, for example, Target Corporation entered into a similar settlement with 47 state AGs that required going-forward compliance with "industry standards" for companies that process payment cards and store customers' personal information. Companies that fail to proactively integrate such standards into their products and services therefore risk hefty civil penalties and costly, lengthy compliance obligations in the event of a data breach.

If you have any questions regarding this client alert, please contact the following attorneys or the attorney with whom you regularly work.

Elizabeth J. Bower
202 303 1252
ebower@willkie.com

James C. Dugan
212 728 8654
jdugan@willkie.com

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Philip F. DiSanto
212 728 8534
pdisanto@willkie.com