THE WALL STREET JOURNAL.

Uber Likely to Face a Barrage of State Legal Action After Breach

By Jeff Stone and Adam Janofsky

Dec. 1, 2017 7:24 a.m. ET

Legal action against ride-hailing app company Uber Technologies Inc. could present a litmus test for state attorneys general looking for a high-profile case they can use to enforce state breach notification laws.

Uber disclosed on Nov. 22 that it paid hackers $100,000 to conceal a 2016 cybersecurity incident in which names, email addresses and mobile phone numbers belonging to some 57 million users around the world were stolen. License numbers of 600,000 Uber drivers were also obtained by outsiders, the company said.

At least five state attorneys general--in New York, Washington, Missouri, Connecticut and Massachusetts--have opened investigations into whether Uber violated state law by failing to inform officials about the incident within a certain amount of time.

“We take this matter very seriously and we are happy to answer any questions regulators may have,” Uber said in a statement. “We are committed to changing the way we do business, putting integrity at the core of every decision we make, and working hard to regain the trust of consumers.”

Forty-eight states have some form of a law that requires breached companies to inform customers about a data breach, particularly if sensitive customer information was involved. The requirements for reporting a breach and the penalties imposed by states can vary widely--Massachusetts can impose fines of $5,000 per violation, for example, while New York and Missouri penalties are capped at $150,000 per breach.

Concealing the breach could violate consumer protection statutes in certain states, and fraud statutes in others.

“Their biggest risk is from state level, and not federal,” said Kenneth Rashbaum, a partner specializing in cybersecurity and compliance at Barton LLP. “State attorneys general are going to want to show they’re serious about their statues. They want to be taken seriously, so they’re going to push very hard on this.”

For Uber, the current challenges could quickly become more complicated if the number of state investigations grows, or if the state attorneys general already investigating Uber join forces.

"We don't make that kind of thing public but it's fair to say I don't view our lawsuit here in Washington state against Uber as the end of our interest in their conduct," Washington State Attorney General Bob Ferguson, who filed suit against Uber Tuesday, told WSJ Pro. "That does not preclude us from taking other steps--and possibly working with other states--to ensure that Uber is held to account for their conduct."

State prosecutors have previously combined their efforts in investigations into data breaches at the privately held hotel chain Hilton Domestic Operating Company Inc., and the public companies Target Corp. and Equifax Inc. In doing so, plaintiffs can share resources such as investigative and legal staffs, seek common ground on which statutes they can proceed under and enjoy other benefits.

"Breach notification laws may be their lead," said Mr. Rashbaum. "States have different times on notifications but they're generally within 60 to 90 days. Some are shorter, and there are reasons for which notification can be delayed but they are very limited, but a year is not a reasonable amount of time."

The incident is quickly shaping up to demonstrate how a data breach can trigger responses from a hodgepodge of regulators and enforcement agencies. It also illustrates how private companies can have more leeway when deciding how to handle a breach in the U.S.

International regulators almost immediately announced probes into the matter. Most recently, data protection officers from throughout the European Union announced a taskforce probe into the company's breach Thursday.

Unlike recent breaches affecting Equifax and other publicly listed companies, Uber had more flexibility in the way it would report a security incident because it's private, though the nature of the breach would have required the organization to take steps it did not appear to, experts said.

"I don't think [the benefits of being private] would be a thing that would keep you from going public, but if you were going public that's the kind of thing you would want to tidy up," said Paige Boshell, partner at Bradley Arant Boult Cummings LLP.

(Jeff Stone writes exclusively for WSJ Pro Cybersecurity. He previously covered privacy, international hacking groups, bug bounties, and a range of related topics at media outlets including the Christian Science Monitor and the International Business Times. Write to Jeff at jeff.stone@wsj.com)

(Adam Janofsky writes about cybersecurity for WSJ Pro, with a specialty in small business. He previously worked at Inc. magazine, Bloomberg News, and managed the WSJ's startup blog. Write to Adam at adam.janofsky@wsj.com.)