Explainer: What the Uber data breach is all about

23 November 2017, by Matt O'brien

This Wednesday, March 1, 2017, file photo shows an exterior view of the headquarters of Uber in San Francisco. Uber paid $100,000 to hackers who stole data on the ride-hailing company's drivers and riders, then kept the massive data breach quiet for a year. This latest stain on Uber's reputation also raises serious questions about ransom payments to hackers, and legal implications as states and federal governments investigate whether Uber violated laws about notifying consumers about their stolen data. (AP Photo/Eric Risberg, File)

When Uber paid a $100,000 ransom so that hackers who broke into its data warehouse would destroy the personal information they stole, it allowed the ride-sharing company to keep a massive breach of 57 million user and driver accounts secret for nearly a year.

Now that secret decision could come to haunt Uber. State and national governments around the world are investigating whether the company violated laws requiring the disclosure of major breaches to customers and legal authorities. It also raises questions about the ongoing practice of paying off hackers, which some experts warn encourages criminals to keep on hacking away at major corporations and the consumers who've entrusted them with their personal information.

—

IS YOUR UBER DATA SAFE?

Uber spokesman Matthew Wing would not comment when asked how the company knows that the hackers destroyed the data they obtained, nor would he comment on other technical or legal issues. Instead, he deferred to new CEO Dara Khosrowshahi's blog posting announcing the breach on Tuesday.

Uber has said that for riders, hackers got only names, email addresses and telephone numbers. They did not get personally identifiable information such as trip details or credit card and Social Security numbers. For about 600,000 U.S. drivers, the hackers obtained driver's license numbers, and the company has offered them free credit monitoring services, the company has said.

—

HOW DID THE BREACH HAPPEN?

The October 2016 hack started at the software repository GitHub, a platform where developers can go to host and review each other's code. Uber hasn't explained how its developers' private account on the site was compromised, but it likely involved some carelessness, said Kyle Flaherty of security firm Rapid7.

"It's like any other account you have," Flaherty said. "Be stringent with your own credentials and be aware of other login credentials that might be inside the repository itself, whether it's in the code or elsewhere." Bloomberg reported that two Uber developers had stashed credentials for the company's data stores in their code on GitHub.

GitHub said Wednesday that the breach was not the result of a failure of its own security, but declined further comment. It also reiterated that it

recommends against storing access tokens, passwords or other authentication or encryption keys in code stored on the site—and warned developers who do so to use extra safeguards to prevent unauthorized access.

—

TO PAY RANSOMS OR NOT

While many security experts have criticized Uber for paying off the hackers with a ransom—which the company later categorized as a more acceptable "bug bounty" awarded to security researchers—others saw the $100,000 payment as a relative bargain that also successfully secured users' data.

"Uber paid $100K to protect 57M people? Good," tweeted Dan Kaminsky, chief scientist at security firm White Ops. "I think people forget the goal is actually to prevent harm. Yeah, those hackers could totally have kept the data. But then, their identities were known, and they knew they might face consequences. Not ideal, welcome to the real."

—

COVERING IT UP

The bigger problem for Uber—and its users—is not so much the payment as the secret maneuvers to keep it hidden, Flaherty said.

"Being open and honest about these types of things is usually the best way to go," he said. "That's the only way this stuff is going to change overall."

Now, though, in addition to yet another hit to its reputation with consumers, Uber faces a mountain of legal hurdles as state prosecutors launched investigations Wednesday and members of Congress called on the Federal Trade Commission to take action.

—

GOVERNMENT RESPONSE

Many U.S. states have laws requiring that companies notify local authorities and consumers if data is stolen. As of Wednesday, attorneys general in New York, Massachusetts and Missouri had announced investigations.

Massachusetts AG Maura Healey, a Democrat, said Wednesday she has requested documents and other information from the ride-hailing service, adding her office is "keeping all criminal and civil options on the table."

The breach will also have repercussions outside the United States.

British officials said Wednesday that any fine against Uber for its large-scale data breach will be higher than usual because the firm did not promptly disclose the hack. Britain's Deputy Information Commissioner James Dipple-Johnstone said that "if U.K. citizens were affected then we should have been notified so that we could assess and verify the impact on people whose data was exposed."

—

Associated Press writers Tom Krisher in Detroit and Bob Salsberg in Boston contributed to this report.