**11/22/17**

*By Susan Grant, Director of Consumer Protection and Privacy, Consumer Federation of America*

The revelation that ride-hailing company Uber experienced a major data breach in October, 2016 and not only kept it secret from the customers and drivers who were affected but even paid the hackers to hush it up is another example of why we need better security for our personal information. While we already have state data breach notice laws, and I'm confident that state authorities will act on any violations that occurred here, the companies that have our personal information should be required to keep it safe, make it unusable if it is hacked, put systems in place to identify breaches quickly, and take the appropriate action to help the victims. Furthermore, there must be strong penalties to hold companies such as Uber accountable.

That's why Consumer Federation of America supports the Consumer Privacy Protection Act of 2017, which was recently introduced by Senator Patrick Leahy. It would require companies to implement privacy and security programs to protect sensitive information about us that they access, collect, use, transmit or store, such as driver's license numbers. They would also have to notify individuals who are affected by the breach without undue delay and provide them with the appropriate identity theft prevention and mitigation services. Just as importantly, businesses that don't comply with the law would be hit where it hurts – in the wallet. The bill would also make it a crime, with the possibility of imprisonment, for concealing a security breach under certain circumstances.

It's time for action to be taken to ensure that companies take data security seriously. This isn't the first data breach at Uber, but it should be the last.

Meanwhile, what should Uber drivers and customers do? The hackers to which Uber paid the ransom promised that they would delete the stolen information, but there's no way of knowing for sure. Uber says that it is going to offer the drivers whose names and license numbers were compromised free identity theft services and credit monitoring. We don't know exactly what the identity theft services will be, but since driver's license information alone can't be used to open

new credit accounts or take over existing ones, credit monitoring isn't going to be much help. According to the Identity Theft Resource Center , the biggest danger is that the license number may be used to cash bad checks or provide a false identity to law enforcement officials. To really help the drivers, Uber should pay for broad monitoring that includes public records and check verification companies, and that provides full fraud resolution services.

Luckily for the Uber customers whose names, email addresses and phone numbers were stolen, at least none of their financial account numbers were involved in the breach. But everyone who has used Uber should be on the alert for calls or emails from crooks pretending to be from Uber, a company hired by Uber, or a law enforcement agency asking for financial or other personal information, supposedly to protect them from fraud.