

Uber CSO Data Breach Charges Provide Lessons On Acceptable Behavior After A Breach

September 3, 2020 - In case you weren't paying attention - and few were - the federal government recently charged former Uber Chief Security Officer Joe Sullivan. His crime? Well according to the government, after a massive 2016 data breach at Uber, Sullivan attempted to cover up the breach entirely. Whether or not that's true will be up to a jury to decide. What is clear though, is that anyone serving in the roll of CSO now knows that avoiding even the appearance of impropriety is critical if you want to avoid legal problems. In Sullivan's case, the charges are felonies.

[Tweet](#)

```
(function() {  
  var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];  
  s.type = 'text/javascript';  
  s.src = 'http://widgets.digg.com/buttons.js';  
  s1.parentNode.insertBefore(s, s1);  
})();
```

```
(function() {  
  var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;  
  po.src = 'https://apis.google.com/js/plusone.js';  
  var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);  
})();
```

Very few people wake up in the morning thinking, "Today is the day I commit a felony!" We're pretty sure that Sullivan falls into that category. He's served as CSO in a number of well-known companies including Facebook. You don't get to that kind of position of responsibility without being serious about your roll.

But in 2016, Uber experienced a massive data breach. Unfortunately, the breach happened just a few days after he had testified to the FTC about a data breach two years earlier. More about that in a minute, but as you will see this timing is an issue with the federal government's case.

After the 2016 data breach and under Sullivan's direction, Uber paid a ransom to the hackers behind the breach to keep the stolen data from being distributed. That's not illegal. In fact, it's an action that was in the best interest of both Uber and their customers because it probably prevented identity theft. But in order to get the ransom, the hackers were asked to sign a binding nondisclosure agreement (NDA). And that's where the problems begin.

According to the government, only Sullivan and Uber's CEO (Travis Kalanick) were aware of the breach or the ransom. Had the NDA only covered information about the ransom, then there probably wouldn't have been a problem. But if it barred any disclosure regarding the breach, then it looks like Sullivan may have been trying to keep the entire thing quiet. And that violates both state and federal law.

The government is also alleging that Sullivan didn't brief Uber's new CEO about the breach when he came on board in 2017; again, making it look like he was keeping the entire incident quiet.

But the government's case has some issues of its own. Specifically, he is being charged with not telling the FTC about

the breach in his testimony. But the testimony actually occurred before the 2016 breach was discovered, so he couldn't have testified about it. That's hardly a cover-up. It isn't even an omission.

Sullivan's intent in requiring the NDA isn't clear. If it was simply to keep the information contained in millions of records from going public, then he didn't do anything wrong. But if he was trying to keep the entire breach secret, that's another story entirely. Either way, what is happening in this case should provide an object lesson to anyone responsible for information security. Make sure that your intentions are clear, especially when you have to act quickly to protect your company and your customers. And put your intentions in writing when you make decisions about any data breach. Not doing so could land you in a pool of boiling water, over which you will have no control.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click [here](#). Registration is easy and free.

Follow ACCESS

Was there an attempted cover up here? That certainly isn't clear at this point but it is worth further investigation.