October 26, 2022

TLP Amber

This week, Hacking Healthcare focuses its attention on what the outcome of the Joseph Sullivan court case might mean for executive liability, the use of bug bounty programs, payments to malicious actors, and incident reporting. In addition to laying out the case and contextualizing what actions the charges stem from, we will outline some steps organizations can take to mitigate the possibility of a similar outcome.

Welcome back to *Hacking Healthcare*.

What Can We Learn From Verdict Against Former Uber CSO Over Incident Handling?

Earlier this month, a jury found Joseph Sullivan, former Chief Security Officer (CSO) of Uber, guilty on two separate counts related to his involvement in Uber's response to a 2016 data breach. The trial has occasionally been referred to as the first time an executive has faced criminal prosecution for a hack, and the verdict has raised serious questions about the legal liability of executives, particularly for CSO/CISOs, for their actions during data breaches.[1] However, closer examination of the evidence and the charges is warranted to effectively assess what lessons should be learned.

For those who have not been following the case closely, let us briefly recap how we got here. In 2015, Sullivan joined Uber as its CSO. During his tenure, Uber disclosed to the Federal Trade Commission (FTC) that it had suffered a data breach in 2014 that involved the unauthorized access of approximately 50,000 consumers' personal information.[2] That disclosure led to the FTC engaging with Uber and launching an investigation into Uber's data security program and practices.[3] This investigation ultimately led to Uber being served "a detailed Civil Investigative Demand on Uber, which demanded both extensive information about any other instances of unauthorized access to user personal information, and information regarding Uber's broader data security program and practices."[4]

Sullivan was the lead for Uber during this investigation and had significant contact with the FTC throughout, including participation in a presentation and testifying under oath. However, ten days after his testimony, Sullivan was contacted by unknown individuals via email who claimed

to have breached Uber's systems and had exfiltrated data relating to 57 million Uber users, including ~600,000 driver's license numbers.[5] Sullivan's actions from this point forward are what appear to have landed him in legal trouble.

Uber was able to confirm that a breach had occurred, and the hackers attempted to extort Uber in return for the stolen data's deletion and their silence. At this point, it appears that Sullivan determined that this interaction should be funneled through Uber's bug bounty program, and it led to Uber paying $100,000 to the still anonymous hackers. In addition to the payment, the hackers signed a non-disclosure agreement "in which the hackers promised not to reveal the hack to anyone, and also contained the false representation that the hackers did not take or store any data in their hack."[6] Evidence was presented that appeared to show that throughout this incident, Sullivan actively limited the number of Uber employees who had knowledge of the breach, including keeping it from Uber's General Counsel.

Uber and Sullivan would continue to work with the FTC for a year without ever mentioning the new 2016 breach. The incident did not come up again until the fall of 2017, when new Uber senior management began to investigate what had happened. Despite Sullivan appearing to have misrepresented the breach to the new senior management, including editing documents that downplayed the scale and sensitivity of the data involved in the 2016 breach, Uber determined that it needed to publicly disclose the incident and remove Sullivan from his position.[7]

In the wake of the incident's publication, Sullivan and Uber faced both state and federal legal troubles. This specific case was brought against Sullivan by the Department of Justice in 2020 and was prosecuted by the Corporate and Securities Fraud Section of the U.S. Attorney's Office, as a result of an investigation by the Federal Bureau of Investigation (FBI). On October 5th, the jury found Sullivan guilty of "obstruction of proceedings of the Federal Trade Commission ("FTC") and misprision of felony."[8]

Action and Analysis
Membership Required

Congress

<u>Tuesday, October 25th:</u>
- No relevant hearings

<u>Wednesday, October 26th:</u>
- No relevant hearings

<u>Thursday, October 27th:</u>
- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

Conferences, Webinars, and Summits

https://h-isac.org/events/

Contact us: follow @HealthISAC, and email at contact@h-isac.org

About the Author

Hacking Healthcare is written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

---

[1] https://www.nytimes.com/2022/10/05/technology/uber-security-chief-joe-sullivan-verdict.html
[2] https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach
[3] https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach
[4] https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach
[5] https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach
[6] https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach
[7] https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach
[8] https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach