Security Newsletter

24 August 2020

Subscribe to this newsletter

Former Uber Security Chief Charged Over Covering Up 2016 Data Breach

The federal prosecutors in the United States have charged Uber's former chief security officer, Joe Sullivan, for covering up a massive data breach that the ride-hailing company suffered in 2016. According to the press release published by the U.S. Department of Justice, Sullivan "took deliberate steps to conceal, deflect, and mislead the Federal Trade Commission about the breach" that also involved paying hackers $100,000 ransom to keep the incident secret.

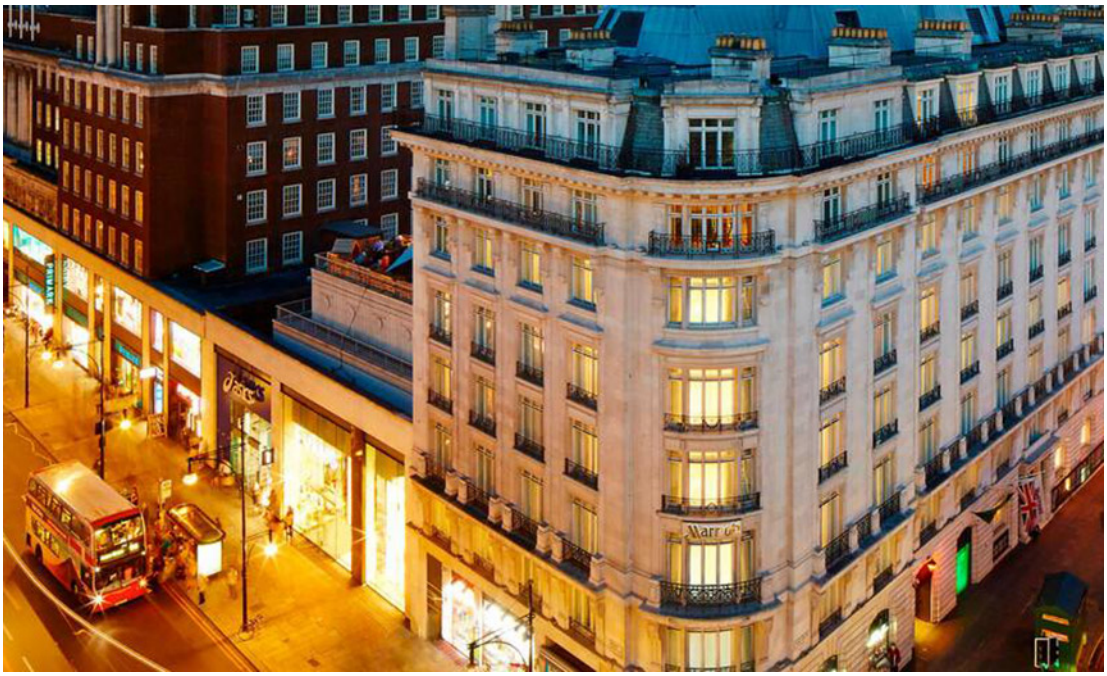
The 2016 Uber's data breach exposed names, email addresses, phone numbers of 57 million Uber riders and drivers, and driver license numbers of around 600,000 drivers. The company revealed this information to the public almost a year later in 2017, immediately after Sullivan left his job at Uber in November. Later it was reported that two hackers, Brandon Charles Glover of Florida and Vasile Mereacre of Toronto, were behind the incident to whom Sullivan approved paying money in exchange for promises to delete data of customers they had stolen.

In 2018, British and Dutch data protection regulators also fined Uber with $1.1 million for failing to protect its customers' personal information during a 2016 cyber attack. Now, if Sullivan found guilty of cover-up charges, he could face up to eight years in prison, as well as potential fines of up to $500,000.

Read More on TheHackerNews

Even More on BankInfoSecurity

Marriott Faces Another Data Breach Lawsuit



Marriott faces another lawsuit, filed in Britain, over the hotel giant experiencing one of the worst data breaches in history. The breach of the Starwood guest reservation system ran from July 2014 to September 2018 - Marriott acquired Starwood in 2016 - and exposed personal information for approximately 339 million customers worldwide. The breach led the ICO - Britain's privacy watchdog - to propose in July 2019 that Marriott be fined £99 million ($131 million) under the EU's General Data Protection Regulation.

"I have filed a data breach group action in the High Court of England and Wales against Marriott International," Bryant says in a Wednesday LinkedIn post. "The action seeks compensation on behalf of millions of hotel guests who made reservations at hotel brands within the Starwood group. This action follows the data breach of hundreds of millions of guest records between July 2014 and September 2018." Marriott already faces class action lawsuits filed in other countries, including lawsuits in Canada. In the United States, a judge combined 11 class action lawsuits into a single one in early 2019. In February, a judge ruled that the lawsuit against Marriott should proceed.

The full amount of damages that Marriott potentially faces is not clear; it will be up to the court to set the per capita sum - should the case go ahead - based on evidence submitted by the hotel chain. In the meantime, British Airways - owned by IAG, for International Airlines Group - also is facing a lawsuit, which was launched in September 2018 by SPG Law, the U.K. branch of U.S. law giant Sanders Phillips Grossman. SPG Law said it was seeking £500 million ($661 million) via its group action. It's not clear what level of compensation victims might receive, although various attorneys have suggested it could be anywhere from £3,000 ($4,000) to £6,000 ($8,000) per victim, or in cases of extreme impact, up to £16,000 ($21,500). Whether any such penalty levels would be approved, however, remains for the court to decide.

Read More on BankInfoSecurity

More #News

- University CISOs say zero trust is the best defense against the existential threat of phishing
- World's largest cruise line operator discloses ransomware attack
- Canada suffers cyberattack used to steal COVID-19 relief payments
- U.S. spirits and wine giant hit by cyberattack, 1TB of data stolen
- Google Chrome will warn users when submitting insecure forms
- Crypto-mining worm steals AWS credentials
- SANS shares details on attack that led to their data breach
- Memory leak in IBM DB2 gives access to sensitive data, causes DoS
- Over 70% of ICS Vulnerabilities Disclosed in First Half of 2020 Remotely Exploitable
- Spotify hit with outage after forgetting to renew a certifficate
- Instacart discloses security incident caused by two contractors
- University of Utah pays $457,000 to ransomware gang
- Hackers Target Defense Contractors' Employees By Posing as Recruiters
- Experian South Africa Suffers Data Breach Affecting Millions; Attacker Identified
- MITRE shares this year's top 25 most dangerous software bugs
- How the shift to remote working has impacted cybersecurity
- Introducing EDR in block mode: Stopping attacks in their tracks
- Microsoft Put Off Fixing Zero Day for 2 Years

#Patch Time!

- Microsoft Issues Emergency Security Updates for Windows 8.1 and Server 2012 R2
- Critical Jenkins Server Vulnerability Could Leak Sensitive Information
- Google fixes major Gmail bug seven hours after exploit details go public

#Tech and #Tools

- Death from Above: Lateral Movement from Azure to On-Prem AD
- Attacking Azure & Azure AD, Part II
- Why you should always scan UDP ports (part 1/2)
- Cross Domain Security
- FritzFrog: A New Generation of Peer-to-Peer Botnets
- Buffer-Overflow Exploit Development Practice
- Rocket.Chat Cross-Site Scripting leading to Remote Code Execution CVE-2020-15926
- HoundSPloit - Search engine for Exploit-DB
- SpaceSiren - Honey Token Manager for AWS
- PowerShell Commands for Incident Response
- Tip: Use EDR to help eliminate the use of password documents in your organizations
- Understanding and Preventing LDAP Injection

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us