Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : bff31a0a | Dec 22, 2022, 08:54 AM

Happy Holidays from Hacking Healthcare

Everyone involved in Hacking Healthcare would like to wish you all a happy holiday season and thank you for another great year. We will be taking next week off for the holidays, but we will be back in January.

This week, Hacking Healthcare examines the FTC's recent decision to take action against both alcohol marketplace Drizly and its CEO, James Cory Rellas, over allegations that the company's security failures led to a large-scale data breach. We briefly break down what happened and attempt to understand how this may create legal precedents to hold top executives responsible for information security best practices. Then, we wrap up this year by reviewing the latest developments in the EU's and United States' attempt to forge a data privacy framework capable of placating EU data privacy laws and U.S. surveillance requirements so that businesses may transfer EU personal data back and forth.

Welcome back to *Hacking Healthcare*.

FTC Penalty Against Drizly's CEO

The Federal Trade Commission ("FTC") issued an order ("Order") against Drizly and its CEO, James Cory Rellas, over their negligence in implementing security measures that led to a data breach, exposing the personal information of 2.5 million consumers.[i] While you might ask, What does an alcohol delivery company have to do with me?, remember that the FTC's purview extends to elements of the healthcare sector, and this regulatory action highlights the importance of not just securing but also disposing of sensitive information. It also raises serious concerns about the FTC's approach to sanctioning executives

.

After suffering a significant data breach in 2018, Drizly officials claimed to have responded to the incident by implementing appropriate security upgrades. Had they implemented policies and processes that required regular review of access permissions, multifactor authentication for all employees with access to code repositories, and scanning of code repositories for unsecured credentials, they might have avoided the FTC's ire when they were breached again in 2020.[ii]

In its proposed order, the FTC imposes a laundry list of security-related obligations and requirements for Drizly to comply with, including destroying unnecessary data, restricting the data that the company can collect and retain, implementing an information security program, and obtaining third-party biennial security assessments for twenty years.[iii] Notably, the FTC's Order does not restrict its requirements to just Drizly, but also imposes the responsibility on its CEO, James Rellas. After repeated data breaches that exposed consumer information, the CEO is being held personally accountable for the latest incident. The FTC is specifically targeting Rellas because despite his claims to have implemented reasonable security practices, he neglected to hire a senior executive responsible for the security of consumers' personal information.[iv]

Misrepresenting the state of its security measures, Rellas will face personal liability, regardless of his choice to stay with Drizly or join another company. For ten years following the final order, Rellas will be required to implement a comprehensive information security program at any organization that collects, uses, stores, or discloses personal information of 25,000 or more consumers where he is either a majority owner, a CEO, or other senior officer with information security responsibilities.[v]

Action & Analysis

Included with H-ISAC Membership

Progress on the EU-U.S. Data Privacy Framework

In July 2020, the Court of Justice of the European Union invalidated the EU-U.S. Privacy Shield, a legal mechanism that allowed EU personal data to be transferred to the United States, on grounds that it did not offer adequate data protections as required by EU law. Since then, while the EU and United States have attempted to find a new path forward to replace the EU-U.S. Privacy Shield, businesses have been operating in a murky legal and regulatory environment, a topic we have covered previously. Thankfully, recent developments may finally signal that relief is in sight.

For those who aren't as familiar with this issue, trans-Atlantic data flows between the EU and United States are a massive driver of business; the Biden administration noted their criticality to the $7.1 trillion economic relationship the two entities share.[vii] However, issues have increasingly bubbled up as the EU and United States have diverged in their approaches to cybersecurity and data privacy.

EU law requires that for a country to be able to receive EU personal data, that country has to have protections in place that offer a level of security and privacy comparable to what is provided to EU citizens. This has been a sticking point with the United States due to the broad surveillance powers the U.S. government retains and has been at the crux of legal challenges that overturned the previous two trans-Atlantic data transfer mechanisms.

On December 13, the European Commission published a draft adequacy decision that came out in favor of the new EU-U.S. Data Privacy Framework. According to its assessment, the United States' implementation of the new framework "ensures an adequate level of protection for personal data transferred from the EU to the US."[viii]

Furthermore, the EU's Justice Commissioner, Didier Reynders, has stated that he believes the framework has a "7 or 8 out of 10" chance of withstanding eventual legal challenges.[ix]

If all goes well, organizations that are currently using Standard Contractual Clauses (SCCs) and other narrow legal mechanisms may have a more straightforward way to legally transfer EU personal data by this summer.[x]

Action & Analysis

Included with H-ISAC Membership

Congress

Tuesday, December 20th:

- No relevant hearings

Wednesday, December 21st:

- No relevant hearings

Thursday, December 22nd:

- No relevant hearings

International Hearings/Meetings

- No relevant meetings

EU –

[i] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023185-drizly-llc-matter
[ii] https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf
[iii] https://www.natlawreview.com/article/ding-dong-ftc-drizly-data-breach-settlement-will-follow-ceo-personally-decade
[iv] https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf
[v] https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million
[vi] https://www.ftc.gov/system/files/ftc_gov/pdf/Statement-of-Chair-Lina-M.-Khan-Joined-By-Commissioner-Alvaro-M.-Bedoya-re-Drizly-final.pdf
[vii] https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/
[viii] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_7632
[ix] https://techcrunch.com/2022/12/13/eu-us-data-privacy-framework-draft-decision/
[x] https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632
[xi] https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf
[xii] https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf

Reference | References

FTC
Health-ISAC
FTC
The National Law Review
Tech Crunch
FTC
Europa Analytics
Whitehouse
Europa Analytics
FTC
Europa Analytics

Report Source(s)

Health-ISAC

Tags

Regulatory, Hacking Healthcare, European Union (EU), FTC

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

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

Hacking Healthcare:

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.