THE CLS BLUE SKY BLOG

COLUMBIA LAW SCHOOL'S BLOG ON CORPORATIONS AND THE CAPITAL MARKETS

https://clsbluesky.law.columbia.edu/2022/12/05/willkie-farr-discusses-personal-liability-for-executives-in-the-wake-of-cyber-incidents/

Willkie Farr Discusses Personal Liability for Executives in the Wake of Cyber Incidents

By Daniel K. Alvarez, Laura E. Jehl, Stefan Ducich and Amal Ibraymi

December 5, 2022

A new and potentially significant tool in regulatory enforcement is emerging for executives whose companies suffer a cybersecurity incident. The Federal Trade Commission ("**FTC**"), in a recently proposed Decision and Order, held James Rellas, the Chief Executive Officer ("**CEO**") of Drizly LLC ("**Drizly**"), personally liable for presiding over the company's failure to implement and apply appropriate information security practices, which led to a data breach resulting in the exposure of 2.5 million consumers' personal information.[1]

The decision marks the first time a senior corporate officer has been found to have personal civil liability arising from a company's security breach. The Drizly Decision and Order, in particular, reinforces a key point made by Commissioner Rebecca Slaughter in recent years: poor cybersecurity practices may no longer be punished only by fines and consent decrees to the companies. Instead, where their actions—or inaction—related to cybersecurity are deemed egregious, company executives may be held personally liable.[2] The potential for civil sanctions against executives is now a key part of the risk analysis for companies and senior leadership as they consider the company's cybersecurity strategy generally, and their decision-making in response to a cybersecurity incident specifically.[3]

Background

The FTC's decision to sanction an executive personally should be considered in light of the specific facts and circumstances of this incident and the role executives played in it.

Drizly is a web-based alcohol ordering and delivery service. In or around July 2020, a threat actor was able to breach a Drizly executive's GitHub account by reusing credentials that had

been acquired via an unrelated breach. Drizly used GitHub for the development, management, and storage of source code, so the threat actor's access to the GitHub account allowed it to analyze the source code for vulnerabilities and modify security settings in the company's AWS database. Moreover, Drizly employees apparently stored credentials in the GitHub repository, despite security guidance from GitHub dating to at least 2013 warning against the practice.

This was the second time Drizly's GitHub account was accessed and leveraged by a threat actor. The first time, in 2018, the threat actor used the access to establish crypto mining operations on Drizly servers and cloud instances. This time, the threat actor was able to leverage these to exfiltrate the personal information of nearly 2.5 million consumers.

Most of the FTC's decision follows the FTC's precedent for data security matters. For example, Drizly is required to implement, maintain, and annually certify an information security program based on principles of data minimization and data retention limits. Where it differs, however, is with respect to Drizly CEO James Rellas, who, according to the FTC, "is responsible for this failure, as he did not implement, or properly delegate the responsibility to implement, reasonable information security practices."[4] By way of example, the FTC's Complaint alleges that he "failed to hire a senior executive responsible for the security of consumers' personal information collected and maintained by Drizly."[5] As a result, the FTC imposes penalties directly on Rellas: for the next 10 years, any future company that handles the data of more than 25,000 people for which he is a majority owner (or for which he serves as "a senior officer with direct or indirect responsibility for information security") must implement an information security program within 180 days of his joining the company.[6]

What Does This Mean for Companies and Executives?

With this action, regulators have signaled the opening of a new front in privacy and cyber enforcement. While there are still many open questions—e.g., how frequently, and under what circumstances, regulators will seek to impose personal liability—it is clear that regulators increasingly see personal liability for executives as a powerful "stick" to encourage good corporate cybersecurity practices. For example, in a joint statement on the Drizly Decision and Order, FTC Chair Lina Khan and Commissioner Alvaro Bedoya emphasize that "holding individual executives accountable . . . can further ensure that firms and the officers that run them are better incentivized to meet their legal obligations."[7]

The Drizly Decision is particularly helpful insofar as it offers some clear examples of the types of actions—or inaction—likely to be considered unfair and deceptive and therefore to violate the FTC Act. In particular, the FTC faulted Drizly—and CEO Rellas—for failing to take steps to protect consumers' data from hackers despite having been alerted to security problems two years prior to the breach and highlighted some of the steps that Drizly could have taken in the wake of the 2018 incident, such as its failure to implement multifactor authentication for employees or to limit access to customer data, and its storing of database login information on an unsecured platform.

The FTC's actions also send a clear signal that the Commission expects executives to address cybersecurity vulnerabilities and undertake associated remediation, and to consistently and proactively monitor (or designate an information security officer to monitor) the company's data protection and cybersecurity practices. Given that, some key takeaways for companies include:

- **Prioritize Security and Privacy as a Business Area:** Companies-including startups-should consider data security and data privacy to be core components of their business. According to the FTC Complaint, Drizly CEO Rellas' liability stems in particular from his failure to appoint an executive responsible for overseeing reasonable information security practices, while focusing instead on other business areas such as finance, legal, marketing, retail, product, and analytics.
- **Button up Internal Processes and Documentation:** Implement a comprehensive data security program, with clear oversight structures to ensure that company data security policies and practices and their incident response strategies are well-documented, comprehensive, clear, and transparent, and which adhere to industry standards.
- **Focus on Data Minimization, Deletion, and Retention:** Companies should aim to collect only the personal information necessary for a given purpose, destroy any unnecessary consumer personal information, and limit the future collection of personal information as regulators increasingly look beyond security control failures to focus on data minimization as a best practice.

Conclusion

The Drizly case is a warning that regulators may be prepared to bring civil charges against both the companies and their executives if companies do not prioritize and reasonably address data protection and cybersecurity issues. As consumer privacy continues to be an FTC priority going forward, companies should be alert for more developments as the Commission finds—and uses—new tools for enforcement.

[1] Press Release, FTC Takes Action against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers (Oct. 24, 2022) (available here).

[2] In an October 2020 speech, Commissioner Slaughter argued that the FTC should incentivize corporate accountability for data privacy practices by investigating the role of executives and, where appropriate, naming the executives in complaints. *See* Remarks of Commissioner Rebecca Kelly Slaughter, FTC Data Privacy Enforcement: A Time of Change, Fed. Trade Comm'n (Oct. 16, 2020) (available here).

[3] The FTC's Decision and Order sanctioning Drizly follows closely on the heels the conviction Joseph Sullivan, the former Chief Security Officer of Uber Technologies, Inc., stemming from his response to the data breach experienced by the company in 2016. *See* Press Release, Dep't of Just., Former Chief Security Officer Of Uber Convicted Of Federal Charges For

Covering Up Data Breach Involving Millions Of Uber User Records (Oct. 5, 2022) (available here).

[4] Complaint, Drizly, LLC, and James Cory Rellas, FTC Docket No. 2023185 at 1 (available here)

[5] *Id*. at 2.

[6] Decision and Order, In the Matter of Drizly, LLC, and James Cory Rellas (available here).

[7] Statement of Chair Lina M. Khan Joined by Commissioner Alvaro M. Bedoya In the Matter of Drizly, Commission File No. 2023185 (Oct. 24, 2022) (available here).

This post comes to us from Willkie, Farr & Gallagher LLP. It is based on the firm's memorandum, "Personal Liability for Executives in the Wake of Cyber Incidents: An Emerging Tool in Cybersecurity Enforcement," dated November 7, 2022, and available here.