UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

Statement of Chair Lina M. Khan
Joined by Commissioner Alvaro M. Bedoya
In the Matter of Drizly
Commission File No. 2023185

October 24, 2022

Today the Commission announced a settlement with the alcohol delivery platform Drizly, LLC, and its CEO, James Cory Rellas, over the company's alleged failure to implement reasonable security policies. According to the complaint, this failure led to several data breaches that exposed the personal information of 2.5 million consumers.

Drizly, a wholly owned subsidiary of Uber, collects and stores a vast amount of user data, including names, physical addresses, geolocation, and alcohol order history. It also stores information about consumers that it purchases from third parties.

The Commission's complaint alleges that in 2018, Rellas and Drizly were alerted to security weaknesses that put its stockpile of consumer data at risk, yet they did not address the problem. According to the complaint, the company neglected to implement basic best practices, such as developing a written data security policy or hiring a qualified employee responsible for data security. Then, in 2020, a hacker was able to access a massive trove of customer data by using login credentials reused by an executive across personal accounts. During this period, Drizly also allegedly made multiple misrepresentations about its data security practices in the privacy policy on its corporate website.

The Commission's proposed order imposes several important conditions to prevent similar failures in the future. It prohibits Drizly from collecting or storing consumer data that is not necessary for pre-specified business purposes. Drizly must also implement a comprehensive security program that features the latest multifactor authentication requirements outlined in recent orders and prevents storage of unsecured credentials on its network or in any cloud-based service. In addition, Drizly must create a public retention schedule for such data, including timeframes for eventual deletion of stored data.

Notably, the order applies personally to Rellas, who presided over Drizly's lax data security practices as CEO. In the modern economy, corporate executives sometimes bounce from company to company, notwithstanding blemishes on their track record.[1] Recognizing that reality, the Commission's proposed order will follow Rellas even if he leaves Drizly. Specifically, Rellas will be required to implement an information security program at future companies if he moves

[1] *See, e.g.*, Rani Molla, *Why Does the WeWork Guy Get to Fail Up?*, RECODE (Aug 17, 2022), https://www.vox.com/recode/2022/8/17/23309756/wework-adam-neumann-flow-andreessen-venture-capital.

to a business collecting consumer information from more than 25,000 individuals, and where he is a majority owner, CEO, or senior officer with information security responsibilities.

Our colleague Commissioner Wilson dissents from the portion of the settlement that personally applies to Rellas. She argues that CEOs of large companies must be allowed to decide for themselves whether or not to pay attention to data security. Respectfully, we disagree. Overseeing a big company is not an excuse to subordinate legal duties in favor of other priorities. The FTC has a role to play in making sure a company's legal obligations are weighed in the boardroom. Today's settlement sends a very clear message: protecting Americans' data is not discretionary. It must be a priority for any chief executive. If anything, it only grows more important as a firm grows.

Today's action will not only correct Drizly's lax data security practices, but should also put other market participants on notice. Limiting the baseline collection and retention of data, as we do here, is a critical tool for protecting Americans from the risks of data breaches, and we will continue to explore remedies centered on limiting the data that is collected or retained in the first place.[2] Finally, holding individual executives accountable, as we also do here, can further ensure that firms and the officers that run them are better incentivized to meet their legal obligations.[3]

***

[2] *See* Press Release, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (Mar. 15, 2022), https://www ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover; Press Release, Fed. Trade Comm'n, Press Release, Fed. Trade Comm'n, FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data (Mar. 4, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive; *see also* Statement of Chair Lina M. Khan Regarding the Report to Congress on Privacy and Security (Oct. 1, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597024/statement_of_chair_lina_m_khan_regarding_the_report_to_congress_on_privacy_and_security_-_final.pdf; Remarks of Chair Lina M. Khan As Prepared for Delivery, IAPP Global Privacy Summit 2022 (Apr. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf; *see generally* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022).

[3] *See* Press Release, Fed. Trade Comm'n, FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data (Sept. 1, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data.