On the WLF Legal Pulse

**Timely commentary from WLF's blog**

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

November 28, 2022

# FTC Action against Data-Breach Victim and its CEO Could Signal New Era of Enforcement

by Gerald A. Stein, Andrea D'Ambra, and Susana Medeiros

The FTC recently took action against both Drizly and its CEO, James Cory Rellas, for violations of Section 5 of the FTC Act that prohibits unfair or deceptive practices. The complaint alleged that Drizly made false statements about their data security practices and had inadequate security that led to a 2020 data breach affecting approximately 2.5 million customers.

This action follows a rise in FTC enforcement actions against companies that have been the victims of a data breach. The FTC has commonly alleged violations that include deceptive data security representations, the failure to implement adequate data security policies and training, and the failure to timely dispose of personal and nonpublic information. Notably in March of this year, the FTC Commission ordered a $500,000 penalty against the owners of CafePress for inadequate security practices and failure to properly investigate a 2019 data breach as part of a consent agreement between the parties.

The Drizly action is unique from other FTC enforcement actions against companies impacted by a cyber event because it names Mr. Rellas individually. The FTC alleges in the complaint that Mr. Rellas was "responsible" for Drizly's purportedly inadequate security practices because he failed to "implement, or properly delegate the responsibility to implement, reasonable information security practices." Specifically, the FTC found that Mr. Rellas failed to hire a senior executive, such as a Chief Technology Officer or Chief Information Security Officer, who would be responsible for the security of consumers' personal information collected and maintained by Drizly.

The FTC's proposed order would require Mr. Rellas to implement and maintain a comprehensive information security program for ten years, and these obligations would travel with him should he leave Drizly to become an owner or senior leader of another covered business. This is intended to ensure that corporate executives like Mr. Rellas who may move to other companies are still held accountable. The Director of the FTC's Bureau of Consumer Protection, Samuel Levine, has said that this "ensures the CEO faces consequences for the company's carelessness."

FTC Commissioner Christine S. Wilson filed a statement dissenting from the FTC's decision to hold Mr. Rellas personally liable. She lists several reasons for her dissent, noting that CEOs must navigate hundreds of business and legal considerations when assessing business risk, and warning against the danger of having regulators substitute senior executives' business judgments for their own. "Companies, not federal regulators, are better positioned to evaluate what risks require the regular attention of a CEO," she said. It is unclear to what extent this dissent may influence the FTC's prosecutorial discretion in future actions.

---

**Gerald A. Stein** is a partner at Norton Rose Fulbright US LLC, and is a member of the firm's Litigation and Disputes Group Antitrust and Competition Group. The opinions expressed herein are his own. **Andrea D'Ambra** is a partner and the firm's US Head of Technology and US Head of eDiscovery and Information Governance. **Susana Medeiros** is an associate and a member of the Information Governance, Privacy, and Cybersecurity team.

The decision to find Mr. Rellas personally liable is uncommon and appears motivated by his purported failure to put a senior executive in charge of ensuring that the company was keeping its data secure, and to ensure monitoring of Drizly's network for unauthorized attempts to access or remove personal data. The FTC may expand upon this in future actions to target senior leadership and find them personally culpable for data security and over-retention of personal information. According to the FTC, "[t]his action is part of the FTC's aggressive efforts to ensure that companies are protecting consumers' data and that careless CEOs learn from their data security failures."

The FTC acted similarly in 2019, when it fined Facebook $5 billion in connection with its privacy practices with Cambridge Analytica. The Commission required CEO Mark Zuckerburg to periodically certify over the next twenty years his company's compliance with privacy reforms that require Facebook to protect the privacy and security of personal information. The FTC, however, did not name Mr. Zuckerberg personally liable, instead assigning this requirement to whomever may be the CEO or President of Facebook. The settlement similarly required Facebook to designate compliance officers responsible for Facebook's privacy program, emphasizing the importance of having dedicated senior personnel focused on these issues. C-Suite executives, as well as other executives and individuals who have oversight over company management, including board members, should take note when evaluating data security risks.

The FTC's proposed order would also require Drizly to destroy unnecessary customer data, restrict the data that the company can collect and retain in accordance with the company's retention schedule, and publicly post its retention schedule. This continues an FTC pattern of focus on data retention and data minimization programs as a means of protecting and limiting the amount of nonpublic information that companies possess.

As part of this increased attention on data minimization, in 2021 the FTC amended its Safeguards Rule, which applies to financial institutions and other covered companies, to require covered institutions to develop procedures "for the secure disposal of customer information . . . no later than two years after the last date the information is used" unless necessary for business or required to be retained. The relevant provision of the law takes effect next week (December 9, 2022), and the FTC is expected to rely on this amendment and increase its focus on perceived unnecessary retention of customer or consumer information. Companies seeking to ensure compliance with this rule should consult with counsel and consider whether their current record retention and information governance programs adequately address the timely disposal of information not subject to business and legal requirements.

The Drizly action should sound a clear alarm bell for companies that the FTC will continue to scrutinize them—and their executives—over their security practices in the fallout of data breaches. We expect that this may prompt companies to target more resources at minimizing their cyber risks and potential enforcement actions, including by maturing their policies and training around data security, maintaining record retention and data minimization programs, and hiring dedicated senior personnel to oversee data security.

 