Concurring and Dissenting Statement of Commissioner Christine S. Wilson

Drizly Matter No. 2023185

October 24, 2022

Today the Commission announces a complaint and settlement resolving allegations that Drizly, LLC and its CEO, James Cory Rellas, violated Section 5 of the FTC Act.

The complaint asserts that Drizly made false statements on its website and in its mobile apps about its information security practices. The Commission also alleges that Drizly engaged in several unreasonable data security practices that led to multiple security breaches, including a hacker's unauthorized download of personal information about 2.5 million consumers.

The FTC has long provided clear guidance to the business community about the fundamentals of sound data security.[1] But, as the complaint details, Drizly failed to develop any written information security standards, policies, or procedures; failed to require unique and complex passwords or multifactor authentication to access source code or databases; failed to terminate employee or contractor access to data once they no longer needed such access; failed to monitor for unauthorized attempts to transfer or exfiltrate consumers' personal information outside company networks; and engaged in other security shortcomings. Notably, simple, readily available, low-cost measures could have addressed Drizly's security shortcomings. I support the complaint against the company and the order provisions that require Drizly to implement numerous data security practices to address the company's missing security safeguards.[2] In particular, my Democratic colleagues and I agree that data minimization plays an important role in a healthy data security program. As Commissioner Slaughter notes in her concurring statement, "hackers cannot steal data that companies did not collect in the first place."

While I support the complaint against the corporate defendant, I do not support holding the individual defendant, Rellas, liable. To seek injunctive relief with respect to a CEO or other principal, the Commission must show only that the individual "participated directly in the deceptive practices *or* had authority to control those practices."[3] Authority to control does not

[1] Fed. Trade Comm'n, *Start with Security: A Guide for Business* (Jun. 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business; Press Release, Fed. Trade Comm'n, Stick with Security: FTC to Provide Additional Insights on Reasonable Data Security Practices (July 21, 2017), https://www.ftc.gov/news-events/press-releases/2017/07/sticksecurity-ftc-provide-additional-insights-reasonable-data.

[2] While I support the settlement against Drizly, I continue to question whether data security orders should remain in effect for 20 years. It is not realistic for the Commission to expect that injunctive relief with respect to this dynamic and rapidly evolving issue will remain relevant and beneficial to consumers for 20 years. *See* Concurring Statement of Commissioner Christine S. Wilson, *In the Matter of* InfoTrax Systems, L.C. and Mark Rawlins, File No. 1623130 (Nov. 19, 2020), https://www.ftc.gov/system/files/documents/public_statements/1553676/162_3130_infotrax_concurring_statement_cw_11-12-2019.pdf.

[3] *FTC v. Ross*, 743 F.3d 886, 892-93 (4th Cir. 2014) (adopting the test for individual liability used by other federal appellate courts, including the First, Seventh, Ninth, Tenth, and Eleventh Circuits). The Commission also can establish liability for monetary relief by showing the defendant "had actual knowledge of the deceptive conduct, was

require the FTC to show a "specific link from [the individual] to the particular deceptive [acts] and instead looks at whether [the individual] had authority to control the corporate entity's practices."[4] This broad standard effectively could enable the Commission to hold individually liable the CEOs of most companies against which we initiate enforcement action.

The Commission traditionally has exercised its prosecutorial discretion and assessed a variety of factors when deciding whether to name a CEO or principal, including consideration of whether individual liability is necessary to obtain effective relief, and the level of the individual's knowledge and participation in the alleged illegal conduct.[5]

The order against Drizly requires the company to implement extensive data security safeguards regardless of whether Rellas is at the helm of the organization. Naming Rellas does not change the injunctive obligations placed on the company to ensure that customers' personal information is protected going forward. Moreover, the case against Drizly makes clear that the FTC expects technology start-ups to start with security and establish reasonable data security practices that grow with the company.

As for knowledge and participation, the number of issues crossing a CEO's desk on any given day is substantial. In most large companies, I would expect CEOs to have little to no involvement with, and no direct knowledge of, practices that are the subject of an FTC investigation. Here, we do not allege that Rellas oversaw day-to-day operations of the company's data security practices, had any data security expertise, or was responsible for decisions about data security policies, procedures, or programs.[6] Instead, we allege that Rellas did not appropriately prioritize hiring a senior executive responsible for privacy and data security. Our complaint notes that he hired other members of the c-suite but not a Chief Technology Officer or Chief Information Security Officer. And for Rellas' failure to prioritize information security over other business obligations, the order imposes on Rellas significant compliance obligations even if he leaves Drizly.[7]

---

recklessly indifferent to its deceptiveness, or had an awareness of a high probability of deceptiveness and intentionally avoided learning the truth." *Id*.

[4] *Id*. at 893.

[5] Many FTC cases involve fraudulent or deceptive conduct by small, closely held companies that essentially serve as the alter egos of their principal or CEO. I support naming the CEO in such a case because the individual defendant is necessary to obtain effective relief and/or to prevent the fraudster from opening and shuttering companies to stay one step ahead of law enforcement. *See* Concurring Statement of Commissioner Christine S. Wilson Regarding FTC v. Progressive Leasing, LLC, File No. 1823127 (April 20, 2020), https://www.ftc.gov/system/files/documents/public_statements/1571921/182_3127_prog_leasing_-_statement_of_commissioner_christine_s_wilson_0.pdf.

[6] *Cf* Complaint, *In re InfoTrax Systems, L.C., a limited liability company, and Mark Rawlins*, Docket No. C-4696 (Dec. 30, 2019) (alleging Rawlins spent eighteen years at a software company, studied computer science in college, "reviewed and approved InfoTrax's information technology security policies, was involved in discussions with clients about data security regularly, and was involved in the company's long-term data security strategy."), https://www.ftc.gov/system/files/documents/cases/c-4696_162_3130_infotrax_complaint_clean.pdf.

[7] The Order binds Rellas to implement an information security program at any future company in which he is a majority owner, CEO, or senior officer with information security responsibilities, where that company collects

By naming Rellas, the Commission has not put the market on notice that the FTC will use its resources to target lax data security practices. Instead, it has signaled that the agency will substitute its own judgement about corporate priorities and governance decisions for those of companies.[8] There is no doubt that robust data security is important. Having a federal data security law would signal to companies, executives, and boards of directors the importance of implementing and maintaining data security programs that address potential risks, taking into account the size of the business and the nature of the data at issue. But CEOs have hundreds of issues and numerous regulatory obligations to navigate. Companies, not federal regulators, are better positioned to evaluate what risks require the regular attention of a CEO. And when companies err in making those assessments, the government will hold them accountable.

Accordingly, I dissent from the inclusion of the individual defendant in the complaint and settlement in this matter.

personal information from at least 25,000 individuals. The Order does not address scenarios in which Boards of Directors, other owners, or higher-ranking executives make it impossible for Rellas to fulfill his obligations.

[8] Then-Commissioner Phillips and I raised similar concerns in our dissents to the FTC's regulatory reviews of the Safeguards Rule. *See* Joint Statement of Commissioners Noah Joshua Phillips and Christine S. Wilson, In the Matter of the Final Rule amending the Gramm-Leach-Bliley Act's Safeguards Rule, File No. P145407 (Oct. 27, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597994/joint_statement_of_commissioners_phillips_and_wilson_in_the_matter_of_regulatory_review_of_the_1.pdf; Dissenting Statement of Commissioner Noah Joshua Phillips and Commissioner Christine S. Wilson, Regulatory Review of Safeguards Rule, File No. P145407 (Mar. 5, 2019), https://www.ftc.gov/system/files/documents/public_statements/1466705/reg_review_of_safeguards_rule_cmr_phillips_wilson_dissent.pdf.