AN A.S. PRATT PUBLICATION
FEBRUARY-MARCH 2023
VOL. 9 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 2** **February-March 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2023–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Federal Trade Commission Settles with Drizly for Alleged Security Failures

By Alexander G. Brown, Kathleen Benway and Ashley Miller*

In this article, the authors explore the implications of a groundbreaking consent order penalizing a company and its chief executive officer for a data breach that allegedly led to the theft of information about millions of consumers.

The Federal Trade Commission (FTC) recently announced a settlement with Drizly LLC, an alcoholic beverage delivery platform, and its chief executive officer after alleged security failures, including reusing the same password, led to a threat actor stealing information about 2.5 million consumers.

THE COMPLAINT

According to the FTC's two-count complaint,[1] Drizly, a subsidiary of Uber Technologies since April 2021, operates a platform that includes tools for verifying the consumer's age; monitoring, tracking, and analyzing orders; and supporting customer service. Drizly's production database environment (the software it uses to operate the e-commerce platform) is hosted by a cloud service provided by Amazon Web Services (AWS) and stores consumer data (like name, email address, postal address, phone numbers, device identifiers, order histories, partial payment information, geolocation information, demographic information, and hashed passwords). In addition to its platform, Drizly utilized the GitHub software platform for the development, management, and storage of its source code that supports Drizly's website and mobile app (and that included Drizly's AWS and database login credentials stored in a GitHub repository that could be used to access Drizly's production environment), which Drizly employees accessed through their personal GitHub accounts.

In April 2018, Drizly provided one of its executives access to the GitHub repositories to participate in a collaborative programming event but did not terminate or monitor the executive's access after the event ended even though it was no longer needed. Nor did Drizly require unique/complex passwords, multifactor authentication, or single

* Alexander G. Brown, a partner in the Atlanta office of Alston & Bird LLP, focuses his complex commercial litigation and investigations practice on high-stakes antitrust, consumer protection, data privacy, cybersecurity, and intellectual property matters. Kathleen Benway, a partner in the firm's office in Washington, D.C., concentrates her practice on government investigations and corporate compliance related to consumer protection issues, including privacy, security, advertising, and FinTech. Ashley Miller, a senior associate in the firm's Atlanta office, focuses her practice on class action defense. The authors may be reached at alex.brown@alston.com, kathleen.benway@alston.com and ashley.miller@alston.com, respectively.

[1] https://www.ftc.gov/system/files/ftc_gov/pdf/202-3185-Drizly-Complaint.pdf.

sign-on to access GitHub. The complaint alleged that to access GitHub the executive used a seven-character alphanumeric password that he also used on other personal accounts. This all came to a head when a malicious actor accessed the executive's GitHub account by reusing credentials from an unrelated breach. With access to the GitHub account, the malicious actor could view source code (to find vulnerabilities in Drizly's software) and access AWS and database credentials. The malicious actor ultimately modified the company's AWS security settings, which provided "unfettered access" to Drizly's production environment and allowed for the exfiltration of more than 2.5 million consumers' personal information. The FTC alleges that this was an unfair information security practice under the FTC Act.

The FTC alleges that CEO James Cory Rellas was responsible for Drizly's security failures because he did not implement or properly delegate the responsibility to implement reasonable security practices. Moreover, not only did Drizly fail to detect the breach itself (instead learning of it from media reports describing the sale of consumer information on dark web forums), Drizly had experienced a similar GitHub breach just two years prior. In the previous breach, a Drizly employee posted AWS credentials to his personal GitHub repository, which led to Drizly's AWS servers being compromised and used to mine cryptocurrency.

The FTC identified two "explicit representations about [Drizly's] information security practices" that it claims led consumers to believe Drizly would use reasonable and appropriate practices to protect their information:

1. From September 1, 2016, Drizly's Privacy Policy stated: "Security. All information we collect is securely stored within our database, and we use standard, industry-wide, commercially reasonable security practices such as 128-bit encryption, firewalls and SSL (Secure Socket Layers)."

2. From October 1, 2019 forward, Drizly's Privacy Policy stated: "Security. We use standard security practices such as encryption and firewalls to protect the information we collect from you."

The FTC concluded that Drizly represented (either expressly or by implication) that it used appropriate safeguards, but "in truth and in fact," it did not.

THE PROPOSED CONSENT ORDER

In addition to the standard language we have all become accustomed to in FTC data security orders, such as a mandatory information security program, third-party assessments, and covered incident reports, the proposed consent order contains a number of notable requirements.

First, there is no civil penalty or other monetary relief. In a post-AMG Capital Management LLC v. FTC[2] world the FTC lacks the hammer it once had in Section 13(b) to leverage monetary relief. While Congress continues to drag its feet on passing a privacy law, the FTC is marching ahead with its privacy rulemaking, which could add to its enforcement arsenal in the form of civil penalty authority, but will take years to finalize. In the meantime, the Drizly consent order sends an important message: the FTC is going to continue privacy-related enforcement actions even with this more limited ability to seek monetary relief.

Second, the FTC has signaled that it will continue to insist on holding individuals liable in some cases. Here, the proposed order will follow CEO Rellas for 10 years. If Rellas is a majority owner of any business that collects consumer information or is employed in certain other high-level roles, he is personally responsible for ensuring that the company implements an information security program. If Rellas were to violate the order while at Drizly (or elsewhere) over the next decade, he would potentially be subject to civil penalties, currently clocking in at $50,120 per violation.

This appears to be the first time that a CEO of a major company has agreed to be bound by an FTC order placing significant obligations related to information security on *any* company where he holds an executive position. In a joint statement,[3] FTC Chair Lina Kahn and Commissioner Alvaro Bedoya said, "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."

Commissioner Rebecca Kelly Slaughter agreed, noting in her statement[4] that naming Drizly's CEO "helps ensure that corporate leadership must take seriously their obligation to safeguard[] customer information." In contrast, Republican Commissioner Christine Wilson dissented[5] because in her mind, he did not have the requisite knowledge and participation necessary to hold an individual liable under the FTC Act.

Finally, the proposed consent order goes beyond standard data collection and retention requirements and shows how the FTC continues to push the boundaries of its authority. With the Drizly order, the FTC does not just require a standard data retention policy and security measures, it demands a company-wide policy of data minimization. Drizly's website and applications must also display its data retention schedule, explaining why it is collecting the consumer information, why it needs the information, and a timeframe for deletion.

---

[2] https://www.supremecourt.gov/opinions/20pdf/19-508_l6gn.pdf.

[3] https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-chair-lina-m-khan-joined-commissioner-alvaro-m-bedoya-matter-drizly.

[4] https://www.ftc.gov/system/files/ftc_gov/pdf/Statement-of-Commissioner-Slaughter-Regarding-Drizly-FINAL.pdf.

[5] https://www.ftc.gov/system/files/ftc_gov/pdf/2023185WilsonDrizlyStatement.pdf.

TAKEAWAYS

While the outcome of the FTC's rulemaking process is uncertain and likely to take years to complete, and the likelihood of a nationwide privacy or data security statute remains in flux, the FTC has signaled a few important points with the Drizly settlement:

- The FTC is going to continue to enforce privacy and data security issues as unfair or deceptive trade practices.
- Individual executive officers will continue to be a target of regulatory scrutiny.
- Companies should train employees on the dangers of reusing passwords across their personal (and business) accounts.
- Companies should consider a data minimization policy on top of data retention standards.
- Companies should heed lessons from prior breaches (which regulators can, and will, use for future enforcement).