King & Spalding
Client Alert

NOVEMBER 9, 2022

FTC Signals Increased Enforcement Effort Against Ineffective Data Security Protocols

For more information, contact:

Marisa Maleck
+1 202 626 9117
mmaleck@kslaw.com

Tamra Moore
+1 202 626 5458
tmoore@kslaw.com

Adam Solander
+1 202 626 5542
asolander@kslaw.com

Hunter McGhee
+1 404 572 4612
hmcghee@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Suite 900
Washington, D.C. 20006
Tel: +1 202 737 0500

With two recent enforcement actions, the Federal Trade Commission (FTC) has shown that administering appropriate data security policies is an area of priority. On October 24, 2022, the FTC announced a Proposed Consent Order (the Drizly Order) against Drizly, a subsidiary of Uber, and its Chief Executive Officer James Cory Rellas, following the company's alleged failure to safeguard consumer data. The Drizly Order requires them to destroy unnecessary data, imposes restrictions on the data the company may collect and retain, and binds them to specific data security requirements.

To facilitate the delivery of alcohol, Drizly collects a wide range of personal information from consumers, including email and postal addresses, phone numbers, unique device identifiers, geolocation information, and third-party data. The FTC alleged Drizly and Rellas were made aware in 2018 of potential security flaws within the company's data security procedures after an employee had posted the company's cloud computing account login information to the software development platform GitHub. Hackers then utilized Drizly's servers to surreptitiously mine cryptocurrency.

Drizly addressed this breach by publicly claiming to have appropriate security systems in place. However, according to the FTC, two years later in 2020, a hacker breached an employee account, accessed Drizly's GitHub login, hacked the company's database, and stole customers' information. The FTC alleged Drizly failed to implement basic security measures following the 2018 breach, despite publicly stating otherwise, stored critical data on an unsecured platform, neglected to monitor security threats, and exposed customers to hackers.

The Drizly Order requires Drizly to destroy any personal data it collected beyond that necessary to provide its services to consumers and report any destruction of data to the FTC. The FTC further ordered Drizly to refrain

from collecting information unless it is necessary for a specific purpose outlined in a retention schedule and to publicly detail the information collected and why such collection is necessary. Lastly, the Drizly Order requires the implementation of a comprehensive data security program to include training employees, designating a supervisor to oversee the program, controlling who can access personal data, and implementing multi-factor authentication. The Drizly Order does not provide any form of consumer redress. Notably, the Drizly Order applies to both Drizly and Rellas personally. Even if Rellas leaves Drizly, he is still bound by the requirements imposed by the Drizly Order.

One week after announcing the Drizly Order, on October 31, 2022, the FTC announced a Proposed Consent Order ("the Chegg Order") against Chegg following the company's alleged failure to implement adequate security measures resulting in four separate data breaches. The Chegg Order requires Chegg to complete a comprehensive restructuring of its data protection practices and give customers access to their data.

Chegg provides a platform through which consumers can rent textbooks, search for scholarships, and receive online tutoring. To facilitate those services, Chegg collects a significant amount of personal information, including consumers' religious affiliation, heritage, date of birth, sexual orientation, disabilities, and parental income. Chegg stored this information utilizing a cloud-based storage system provided by Amazon Web Services. The FTC alleged the company created multiple security risks by having an insufficient security policy. For example, Chegg did not encrypt collected data, require multi-factor authentication to access the data, adequately train employees, or have a process for deleting customer and employee data when there was no longer a business need to maintain it.

According to the FTC, these lax security protocols led to four separate security incidents. Three of those incidents were successful phishing attacks which allowed hackers direct access to employee direct deposit payroll information, consumer financial and medical information, and employee birthdates and Social Security numbers found on their W-2 forms. The remaining incident involved a former Chegg contractor who used Chegg's credentials to access personal information in Chegg's cloud storage and subsequently post the information on a public website.

The FTC lodged a complaint against Chegg alleging the company failed to take precautionary steps to prevent or detect threats to consumer and employee data. In settling the case, Chegg agreed to overhaul its data protection practices. The Chegg Order requires Chegg follow a schedule describing the information it collects, why it collects the information, and when it will delete the data. Chegg must allow customers to access the collected information and honor any consumer requests to delete the data and must implement two-factor authentication methods to help protect consumer and employee accounts. The Chegg Order does not provide any form of consumer redress.

These recent actions serve as a reminder that addressing data security failures is an area of priority for the FTC. Not only is the FTC increasing its scrutiny on company data security procedures, but it also makes clear that corporate executives bear some responsibility in implementing appropriate security measures. Companies should employ foundational data protection methods, such as multi-factor authentication, data encryption, and security stress testing. In the event of a security incident, companies should respond immediately and definitively through comprehensive review of existing security protocols. Additionally, companies should create and continually implement in-house training procedures to prepare employees for data security incidents.

About King & Spalding's Data, Privacy and Security Practice

The firm's Data, Privacy and Security practice includes over 80 lawyers and professionals based in many of the firm's offices and encompasses global data protection legal issues faced by multinational organizations, including data protection, crisis management in responding to internal and external data, privacy and security incidents, information governance and compliance, and defending clients in enforcement proceedings and litigation. We are "boots on the

ground" crisis managers, deploying our incident response team, when needed, to manage the fast-moving logistics and coordinate across work streams during the initial hours and days of a privacy or security incident.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 23 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE
ATLANTA	CHICAGO	GENEVA	MIAMI	RIYADH	TOKYO
AUSTIN	DENVER	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
BRUSSELS	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	