Armstrong Teasdale

January 9, 2023 • Advisory • www.atllp.com

RECENT FEDERAL, STATE ACTIONS SIGNAL INCREASED SCRUTINY FOR EXECUTIVES ON CYBERSECURITY COMPLIANCE

Earlier this year, the Federal Trade Commission (FTC) took action against online alcohol marketplace Drizly and CEO James Cory Rellas over allegations that the company's security failures led to a data breach exposing the personal information of 2.5 million consumers. The FTC's order alleges that Drizly and Rellas were alerted to security problems two years prior to the breach, yet failed to take steps to protect consumers' data from hackers.

The order significantly limits what information the company can collect and requires significant data minimization practices. Aside from those remarkable actions, the FTC's order is unique because it not only applies directly to the company, but also its CEO individually. By tying the CEO to the order as an individual, the FTC will require him to abide by the order even if he were to move to a new company. This is good evidence that the FTC is further focusing on the requirement for board members to be personally involved in the cybersecurity posture of a company.

This increased focus on executive personnel in connection with data security concerns is not relegated only to the federal space. The New York Department of Financial Services' (NYDFS) recent proposed amendments to its Cybersecurity Regulations also evidence an increased focus on board oversight of cybersecurity programs. On Nov. 9, 2022, the proposed second amendment to 23 NYCRR Part 500 (DFS Cybersecurity Regulation) was published in the New York State Register. The proposed amendments would require a covered entity to submit a written statement to the superintendent certifying that the covered entity has complied throughout the year with the requirements set forth in Part 500. This certification must be based upon data and documentation sufficient to accurately determine and demonstrate full compliance, and must be signed by the covered entity's highest-ranking executive and its Chief Information Security Officer (CISO). If the entity does not have a CISO, the certification must be signed by the highest-ranking executive and by the senior officer responsible for the cybersecurity program of the covered entity. These certifications must be maintained by the covered entity for at least five years. The public comment period for these amendments

PEOPLE
Jeffrey Schultz, CIPP/US

SERVICES AND INDUSTRIES
Data Innovation, Security and Privacy

ends on Jan. 9, 2023.

Based on both the action against Drizly and proposed changes to NYDFS's Cybersecurity Regulations, executives and board members—including those who do not have a direct responsibility for cybersecurity—are under closer scrutiny and ought to pay attention to and stay abreast of their company's cybersecurity programs. We expect this pattern to continue in other state and federal laws and regulations.

Our Data Innovation, Security and Privacy team is actively monitoring for developments in this space and has deep experience helping clients navigate complex regulatory issues related to cybersecurity. Contact your regular AT lawyers or one of the authors listed below for proactive guidance specific to your organization.