PUBLICATION

Privacy in 2023: Management and Officer Liability for Privacy and Data Security Programs

Authors: Alisa L. Chestler
January 24, 2023

If your management team and board of directors are not talking often about cyber liability and risk management, they will be soon.

As a matter of both corporate and individual liability, recent enforcement makes it clear that management cannot rely on generic privacy policy language at the expense of meaningful operations supporting the statements it posts and publicizes.

As an example, the Federal Trade Commission (FTC) announced an enforcement action against the online alcohol marketplace Drizly in late October 2022. This FTC action comes after Drizly's data breach in 2020 when internal data security failures affected the information of 2.5 million customers.

FTC enforcement in privacy is common, but their new focus on management's role in privacy and information security is unprecedented. On January 10, the FTC finalized the Drizly consent order requiring the company to implement and maintain a data protection program, which is a common outcome of any privacy-related consent order. What has been less common to date, however, was the FTC's requirement that Drizly's Chief Executive Officer, James Cory Rellas, implement an information security program at any future companies he works for that meet certain specifications.

In this unprecedented move, Rellas will be required to ensure that any business with which he is involved that is in possession of the personal data of more than 25,000 consumers and he (i) holds a majority interest, (ii) serves as CEO, or (iii) holds a management position, implements and maintains a formal information security management program. The FTC press release in October specifically underscored this mandate, with FTC Bureau of Consumer Protection Director Samuel Levine stating that the order not only "restricts what the company can retain and collect going forward," but also ensures the CEO "faces consequences for the company's carelessness."

Accordingly, the FTC's final decision is fairly substantial in its depth and breadth. The FTC highlights two key violations by Drizly:

(i) failure to implement readily available, low-cost data safeguards and

(ii) using the company's website to misrepresent compliance with commercially reasonable security practices.

Within these violations, the FTC points to the absence of written policies and procedures at the company, such as those requiring employee training, and neglecting to place qualified professionals at the helm of a data security program. Drizly also failed to implement certain other standard safeguards and policies, which allowed for faulty encryption technology, poor credential management, absence of multi-factor authentication, and inability to monitor for the exfiltration of data. The FTC found that Rellas should have been aware of these issues, especially given a prior incident that served as constructive notice to Rellas of Drizly's inadequate privacy and security practices.

Now, Drizly is tasked with implementing an information security program, including policies and procedures for:

(i) specifying data retention, destruction, and minimization limits;

(ii) introducing data access controls;

(iii) routinely testing safeguards;

(iv) training employees; and

(v) creating measures to prevent storage of unsecured access keys or credentials.

Further, this program will be subject to biennial third-party assessments to ensure its ability to protect personal information.

Moving forward, the FTC's ongoing monitoring of Drizly and Rellas serves to alert companies to its expectations for the development of data protection programs and accountability for misrepresentations of compliance with reasonable security practices.

The bottom line for your company and its management and officers:

Management cannot rely on a one-size-fits-all privacy policy. Businesses – and their individual leaders – must accept responsibility for evaluating the company's operations and adopting meaningful operations that support the statements it posts and publicizes.

If you have questions or want to know more about how to implement a robust privacy and data security program, please contact Alisa Chestler or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.