FTC Holds Corporate Executive Personally Liable for Cybersecurity Failures Million

On Jan. 10, 2023, the Federal Trade Commission (FTC) finalized its order against online alcohol marketplace, Drizly, and its CEO, James Cory Rellas for failing to implement security safeguards that led to a data breach in 2020 that exposed 2.5 million users' personal information. Under the order, Drizly must implement data security measures that include the minimization, deletion, and retention of personal information. Notably, the order extends to any future employment of Rellas for the next 10 years.

The FTC's decision marks the first time it has held an executive personally liable for failing to follow cybersecurity and data privacy compliance. Under the Federal Trade Commission Act, a person can be held individually liable when the individual: (1) participated directly in the deceptive trade practice or had had authority to control them; and (2) had knowledge of the deceptive conduct. The main factor that could lead to individual liability is when an executive has awareness of cybersecurity and data privacy practices within the organization.

FTC Complaint

According to the FTC's complaint, in 2018 both Drizly and Rellas were notified about security vulnerabilities prior to the data breach but failed to adequately mitigate these vulnerabilities. Specifically, Drizly did not securely store database login credentials, which allowed a malicious actor to gain access to and steal the data of those 2.5 million people. Moreover, Rellas neglected to hire a senior executive responsible for managing the security of consumers' personal information collected and maintained by Drizly. The FTC also alleged that Drizly and Rellas:

- Failed to implement basic security measures such as two-factor authentication, access controls and employee training.
- Stored sensitive login credentials on the unsecured platform, GitHub despite well documented security risks concerning the platform.
- Neglected to monitor network for external threats of unauthorized access.
- Exposed customers to hackers and identity thieves when the information exfiltrated during the breach was put up for sale on the dark web.

FTC Enforcement Action

The order outlines several requirements that Drizly and Rellas must undertake. Drizly is required to:

- Delete all personal information collected that is not essential to it providing services and products to its consumers and notify the FTC of what information was deleted.
- Refrain from collecting any personal information unless its specific purpose is outlined in Drizly's publicly available retention schedule.
- Publicly disclose the personal information it collects and reasons for collecting.

- Implement an information security system, which should include measures such as an employee to oversee the program, a procedure for when a data breach occurs, and employee training.
- Hire a third-party to conduct biennial security assessments for the next 20 years.

Significantly, if Rellas becomes employed at a different company, he is required to implement an information security program in any business that collects personal information of more than 25,000 individuals, where he is a majority owner or is an officer that has security responsibilities.

Takeaways

This decision is notable as it came soon after Uber's former Chief Security Officer's conviction for covering up a ransomware attack during an FTC investigation. Most recently, the FTC amended its complaint against Amazon employees for deceptive sign-up and cancellation processes for Prime to include three executives. Additionally, in their complaint, the FTC alluded to their authority to hold executives liable even when they do not personally engage in the unfair or deceptive practices of the company. Both decisions are indicative of a trend in the FTC holding executives liable for their decisions and efforts regarding cybersecurity and data privacy compliance.

Therefore, executives should take action to mitigate any security risks if they have knowledge regarding vulnerabilities in their organization's cybersecurity and data privacy practices. Additionally, executives should look to see whether there are reasonable information security safeguards in place. These safeguards could include having policies specifying data retention and destruction, training employees, and routinely reviewing policies and procedures.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters, including regulatory reporting. If you have any questions regarding being held individually liable for your organization's cybersecurity and privacy procedures, please contact Jessica Copeland, CIPP/US, Mario Ayoub or any attorney in Bond's cybersecurity and data privacy practice.

**Special thanks to Associate Trainee Victoria Okraszewski for her assistance in the preparation of this blast. Victoria is not yet admitted to practice law.*

BOND SCHOENECK & KING ATTORNEYS