**Analysis of Proposed Consent Order to Aid Public Comment**
***In the Matter of* Drizly, LLC and James Cory Rellas, File No. 2023185**

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a Proposed Consent Order ("Proposed Order") from Drizly, LLC ("Drizly" or "Corporate Respondent") and James Cory Rellas ("Rellas" or "Individual Respondent"), individually and as an officer of Drizly (collectively, "Respondents").

The Proposed Order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's Proposed Order.

This matter involves Respondents' data security practices. Drizly operates an e-commerce platform that enables local retailers to sell alcohol online to consumers of legal drinking age and stored personal information for more than 2.5 million consumers. Respondents engaged in a number of unreasonable data security practices which caused or are likely to cause substantial consumer injury. In addition, Corporate Respondent made a number of misrepresentations to consumers in its privacy policies about the measures it took to protect consumers' personal information.

The Commission's proposed two-count complaint alleges that Respondents have violated Section 5(a) of the Federal Trade Commission Act.

First, the complaint alleges that Respondents have engaged in a number of unreasonable security practices that led to a hacker's unauthorized download of personal information about 2.5 million consumers. The complaint alleges that Respondents:

- Failed to develop adequate written information security standards, policies, procedures, or practices; assess or enforce compliance with the written standards, policies, procedures, and practices that it did have; and implement training for employees (including engineers) regarding such standards, policies, procedures, and practices;

- Failed to securely store AWS and database login credentials, by including them in GitHub repositories, and failed to use readily available measures to scan these repositories for unsecured credentials (such as usernames, passwords, API keys, secure access tokens, and asymmetric private keys);

- Failed to impose reasonable data access controls such as: (1) unique and complex passwords or multifactor authentication to access source code or databases; (2) enforcing role-based access controls; (3) monitoring and terminating employee and contractor access to source code once they no longer needed such access; (4)

restricting inbound connections to known IP addresses; and (5) requiring appropriate authentications between Drizly applications and the production environment;

- Failed to prevent data loss by monitoring for unauthorized attempts to transfer or exfiltrate consumers' personal information outside the company's network boundaries; continually log and monitor its systems and assets to identify data security events; and perform regular assessments as to the effectiveness of protection measures;

- Failed to test, audit, assess, or review its products' or applications' security features; and conduct regular risk assessments, vulnerability scans, and penetration testing of its networks and databases; and

- Failed to have a policy, procedure, or practice for inventorying and deleting consumers' personal information stored on its network that was no longer necessary.

The complaint alleges that Respondents could have addressed each of the failures described through well known, readily available, and relatively low-cost measures.

The complaint alleges that Respondent's failures caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. Such practice constitutes an unfair act or practice under Section 5 of the FTC Act.

Second, the complaint alleges that Corporate Respondent made false statements on its corporate website and in its mobile apps about its information security practices. Specifically, Corporate Respondent misrepresented to consumers the information it collects from consumers is securely stored and protected by commercially reasonable security practices. The complaint alleges that Corporate Respondent's actions constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act.

The Proposed Order contains injunctive provisions addressing the alleged unfair and deceptive conduct in connection with Respondent's sale of dealer management system software and services. Part I of the Proposed Order prohibits Corporate Respondent from misrepresenting the privacy and security measures it uses to protect consumers' information and privacy.

Part II of the Proposed Order requires Corporate Respondent to delete within 60 days any "Covered Information" that is not being used or retained in connection with providing products or services to consumers, and to provide written statements to the Commission describing the specific deletion of any such "Covered Information." In addition, Corporate Respondent must refrain from collecting or maintaining any future "Covered Information," if the purpose is not necessary for specific purposes described in a retention schedule.

Part III of the Proposed Order requires Corporate Respondent to create and display on its website and apps a retention schedule for any "Covered Information" it collects, maintains, uses, discloses, or provides access. The schedule must provide a purpose for the information collection, the business need for any retention, and a timeframe for eventual deletion.

Part IV of the Proposed Order requires Corporate Respondent to implement an Information Security Program, requiring among other things:

- Training in secure software development principles, including secure engineering and defensive programming concepts;
- Measures to prevent the storage of unsecured access keys or other unsecured credentials;
- Implementation of data access controls;
- Risk assessment of source code and controls such as software code review; and
- Use of non-SMS based multi-factor authentication for employees, and offering multi-factor authentication as an option for consumers.

Corporate Respondent must also obtain initial and biennial third-party assessments of its Information Security Program implementation (Part V), cooperate with the third-party assessor performing such assessments (Part VI), have a senior corporate manager or corporate officer make annual certifications regarding Corporate Respondent's compliance with the Proposed Order's data security requirements (Part VIII), and report to the Commission any event involving consumers' personal information that constitutes a reportable event to any U.S. federal, state, or local government authority (Part IX).

Part VII of the Proposed Order requires Individual Respondent James Cory Rellas, for a period of ten years, for any business that he is a majority owner, or is employed or functions as a CEO or other senior officer with responsibility for information security, to ensure the business has established and implements, and thereafter maintains, an information security program.

Parts X-XIII of the Proposed Order are standard scofflaw provisions requiring: acknowledgment of the Order to be delivered for ten years to corporate officers and employees engaged in the conduct related to the order; a compliance report to be submitted within one year of the order and after corporate changes; recordkeeping requirements that last twenty years; and the submission, upon request, of additional reports and records for compliance monitoring.

Part XIV of the Proposed Order provides that the order terminates 20 years after its issuance or 20 years after the latest complaint filed in federal court alleging a violation of the order.

The purpose of this analysis is to aid public comment on the Proposed Order. It is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify in any way the Proposed Order's terms.