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 polare d-2 (t)-2 (y pr)3 (a)-6 (c)4 (t)-2 (i)-0

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.