2023185

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Noah Joshua Phillips
Rebecca Kelly Slaughter
Christine S. Wilson
Alvaro M. Bedoya

In the Matter of **DRIZLY, LLC, a Limited Liability Company,** **and** **JAMES CORY RELLAS, individually, and as an officer of DRIZLY, LLC.**	**DECISION AND ORDER** **DOCKET NO.**

DECISION

The Federal Trade Commission ("Commission") in

conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondents are:

    a.

5. "**Delete**" "**Deleted**" or "**Deletion**" means to remove Covered Information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

6. "**Individual Respondent**" means James Cory Rellas.

7. "**Relevant Business**" means any business other than a Covered Business that collects, uses, discloses, or stores Covered Information from 25,000 or more individual consumers.

8. "**Respondents**" means the Corporate Respondent and the Individual Respondent, individually, collectively, or in any combination.

9. "**User**" means an individual consumer from whom Covered Business has obtained information for the purpose of providing access to a Respondent's products and services.

Provisions

I. Prohibition Against Misrepresentations

IT IS ORDERED that Corporate Respondent and Corporate Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, must not misrepresent in any manner, expressly or by implication:

A. The extent to which Corporate Respondent collects, uses, discloses, maintains, Deletes, or permits or denies access to any Covered Information;

B. The extent to which Corporate Respondent

B. Refrain from collecting or maintaining any Covered Information not necessary for the specific purpose(s) provided in the retention schedule required under Provision III entitled Data Retention Limits.

Provided, however, that any data that Corporate Respondent is required to Delete or destroy pursuant to this Provision may be retained if required by law, regulation, court order, contractual obligations requiring Corporate Respondent to maintain records on behalf of retailers to document the retailers' compliance with state or local liquor regulations, or legal process, including as required by rules applicable to the safeguarding of evidence in pending litigation.

III. Data Retention Limits

IT IS FURTHER ORDERED that Corporate Respondent, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must:

A. Within 60 days of issuance of this Order, document, adhere to, and make publicly available on its website(s) or app(s), a retention schedule for Covered Information, setting forth: (1) the purpose or purposes for which each type of Covered Information is

implement, and operate a Covered Business' products or services or that are otherwise responsible for the security of Covered Information;

3. Technical measures, standards, procedures, and policy provisions to prevent the storage of unsecured access keys or other unsecured credentials on a Covered Business' network or in any cloud-based services;

4. Policy provisions and, to the extent possible, technical measures requiring employees, contractors, or third parties to secure any accounts with access to a Covered Business' information technology infrastructure by: (a) using strong, unique passwords; and (b) using multi-factor authentication whenever available;

5. Requiring multi-factor authentication methods for all employees, contractors, and affiliates in order to access any assets (including databases) storing Covered Information. Such multi-factor authentication methods for all employees, contractors, and affiliates shall not include telephone or SMS-based authentication methods and must be resistant to phishing attacks. A Covered Business may use widely-adopted industry authentication options that provide at least equivalent security as the multi-factor authentication options required by this sub-provision, if approved in writing by the Commission;

6. Requiring multi-factor authentication methods be provided as an option for consumers. Any information collected from consumers at the time they select to use multi-factor authentication may only be used for authentication purposes and no other purpose;

7. Technical measures, standards, procedures, and policy provisions to: (a) log and monitor access to repositories of Covered Information in the control of a Covered Business; (b) limit access to Covered Information by, at a minimum, limiting employee and service provider access to what is needed to perform that employee's or service provider's job function; (c) grant and audit varying levels of access based on an employee's need to know; and (d) periodically monitor and terminate employee and contractor accounts following inappropriate usage or termination of employment;

8. Technical measures, standards, procedures, and policy provisions to control data access for all assets (including databases) containing Covered Information or resources containing proprietary (*i.e.*, non-open source) source code repositories, including, at a minimum: (a) restrictions of inbound connections to those originating from approved IP addresses; (b) requiring connections to be authenticated and encrypted; and (c) periodic audits of account permissions;

9. Technical measures, standards, procedures, and policy provisions to: (a) monitor and log transfers or exfiltration of Covered Information outside each Covered Business' network boundaries; (b) monitor and log data security events and other anomalous activity; and (c) verify the effectiveness of monitoring and logging;

C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Corporate Respondent has implemented and maintained the Mandated Information Security Program for Covered Businesses; (2) assessment of the effectiveness of the Corporate Respondent's implementation and maintenance of sub-Provisions A-I of the required Mandated Information Security Program for Covered Businesses; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Mandated Information Security Program for Covered Businesses.

VII. Mandated Information Security Program for Certain Businesses of the Individual Respondent

IT IS FURTHER ORDERED that, for 10 years after issuance of this Order, Individual Respondent, for any Relevant Business that he is: 1) majority owner; or 2) employed or functions as a Chief Executive Officer or other senior officer with direct or indirect responsibility

F. Assesses, at least once every 12 months, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Covered Information, and modify the Business ISP based on the results;

G. Tests and monitors the effectiveness of the safeguards in place at least once every 12 months, and modifies the Business ISP based on the results. Such testing and monitoring

B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "*In re* Drizly, LLC and James Cory Rellas, FTC File No. 2023185."

IX. Covered Incident Reports

IT IS FURTHER ORDERED that, within 10 days of any notification to a United States federal, state, or local entity of a Covered Incident, each Covered Business must submit a report to the Commission. The report must include, to the extent possible:

A. The date, estimated date, or estimated date range when the Covered Incident occurred;

B. A description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;

C. A description of each type of information that was affected by the Covered Incident;

D. The number of consumers whose information was affected by the Covered Incident;

E. The acts that each Covered Business has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

F. A representative copy of each materially different notice sent by each Covered Business to consumers or to any U.S. federal, state, or local government entity regarding the Covered Incident.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "*In re* Drizly, LLC and James Cory Rellas, FTC File No. 2023185."

X. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondents obtain acknowledgments of receipt of

B. For 10 years after the issuance date of this Order, Individual Respondent for any business that such Respondent, individually or collectively with any other Respondent is the majority owner or controls, directly or indirectly, and Corporate Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives with managerial responsibilities for a Covered Business' data security, collection of consumer information, and decision-making about the use of consumer information; (3) the employee(s) having primary responsibility for a Relevant Business' data security, collection of consumer information, and decision-making about the use of consumer information; and (4) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondents delivered a copy of this Order, Respondents must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

XI. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondents make timely submissions to the Commission:

A. One year after the issuance date of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which:

1. Each Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) good85 -Respondtu,1ely meaniaf3.ust submit a (bo5d[Onvolvend s) having primary)Tj0.10

title, role, responsibilities, participation, authority, control, and any ownership; and (d) explain whether or not any business identified in sub-part (b) is a Relevant Business.

B. Each Respondent must submit a complianc

majority owner or controls directly or indirectly must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;

B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name, addresses, telephone numbers, job title or position, dates of service, and (if applicable) the reason for termination;

C. Copies or records of all consumer complaints related to information security, privacy, or identity theft whether received directly or indirectly by Corporate Respondent, such as through a third party, and any response;

D. A copy of each unique advertisement or other marketing material of Corporate Respondent containing a representation subject to this Order;

E. A copy of each widely disseminated and materially different representation by Corporate Respondent that describes the extent to which Corporate Respondent maintains or protects the privacy, security, availability, confidentiality, or integrity of any Covered Information, including any representation concerning a change in any website or other service controlled by Corporate Respondent that relates to privacy, security, availability, confidentiality, or integrit

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED: