**2023185**

**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

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

| | |
|---|---|
| **In the Matter of**<br><br>**DRIZLY, LLC, a Limited Liability Company,**<br>**and**<br>**JAMES CORY RELLAS, individually, and as an officer of DRIZLY, LLC.** | **DOCKET NO. C-4780** |

## COMPLAINT

The Federal Trade Commission ("FTC"), having reason to believe that Drizly, LLC, a limited liability company, and James Cory Rellas, individually and as an officer of Drizly, LLC (collectively "Respondents"), violated provisions of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Drizly, LLC ("Drizly") is a Delaware limited liability company with its principal place of business at 501 Boylston Street, Boston, MA 02216. Until October 13, 2021, Drizly was a subsidiary of The Drizly Group, Inc., a holding company. On October 13, 2021, Drizly, LLC became a wholly-owned subsidiary of Uber Technologies, Inc. ("Uber").

2. Respondent James Cory Rellas ("Rellas"), is the Chief Executive Officer ("CEO") of Drizly, LLC. Individually or in concert with others, he had the authority to control, or participated in, the acts and practices alleged in this complaint.

3. Respondents' acts and practices as alleged in this Complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

## Summary of the Case

4. Drizly failed to use appropriate information security practices to protect consumers' personal information. These failures allowed a malicious actor to access Drizly's consumer database and steal information relating to 2.5 million consumers, as described in greater detail below. Rellas is responsible for this failure, as he did not implement, or

properly delegate the responsibility to implement, reasonable information security practices. Indeed, as CEO of Drizly prior to and during the breach, Rellas hired senior executives dedicated to finance, legal, marketing, retail, human resources, product, and analytics, but failed to hire a senior executive responsible for the security of consumers' personal information collected and maintained by Drizly.

## Drizly's Business Model and Operations

5. Drizly operates an e-commerce platform that enables local retailers to sell alcohol online to consumers of legal drinking age. Retailers choose the products to offer and the prices to charge on the platform. When a consumer places an order through Drizly's website or one of Drizly's mobile apps, the retailer accepts the order and facilitates delivery of the purchase.

6. Drizly's platform includes tools to verify a consumer's age; monitor, track, and analyze orders; and support customer service. The platform also collects and stores both personal information that consumers provide and information that it automatically obtains from consumers' computers and mobile devices.

7. Drizly was founded in 2012 and now has more than 360 employees. The company maintains a headquarters in Boston, Massachusetts and an office in Denver, Colorado. It advertises itself as North America's "largest online marketplace for alcohol," partnering with more than 4,000 retailers across 1,600 urban and suburban markets. Drizly claims that it facilitates sales of alcohol for delivery in more than 33 states and the District of Columbia. It also claims that its retail partners saw average growth in 2020 of 350%, with an average monthly number of orders of more than 230 per store.

8. Rellas has been Drizly's Chief Executive Officer since August 2018. He was previously Drizly's Chief Operating Officer and is a co-founder of Drizly. At all times relevant to the allegations in this Complaint, Rellas had the authority to control, or participated in, Drizly's information security practices.

## Drizly's Information Technology Infrastructure

9. Drizly uses a third-party service called the Amazon Relational Database Service ("Amazon RDS") to host its production database environment (the software Drizly uses to operate its e-commerce platform). Amazon RDS is a cloud service provided by Amazon Web Services ("AWS").

10. Drizly's production environment includes a variety of applications and databases, some of which store personal information. These databases contain, among other things, names, email addresses, postal addresses, phone numbers, unique device identifiers, order histories, partial payment information, geolocation information, and consumer data (including, *e.g.*, income level, marital status, gender, ethnicity, existence of children, and home value) purchased from third parties. The databases also contain passwords that were hashed—converted into new values so as not to store the password itself in the database. The passwords were hashed using the bcrypt function or MD5, the latter of which is cryptographically broken, and widely considered insecure. This personal

information can be misused to facilitate identity theft and other consumer harm. Drizly's databases contain some or all of this personal information for more than 2.5 million consumers.

11. Drizly also uses the GitHub software platform ("GitHub") for the development, management, and storage of source code that supports the Drizly website and mobile apps. GitHub facilitates collaboration among developers, allowing them to store and share project files, including images, spreadsheets, and data sets, as well as the histories of all source code changes, in "repositories." Through its GitHub account, Drizly maintains a number of repositories that hold company data and projects, and which at one point improperly held AWS credentials, which could be used to access the company's production environment.

12. Drizly employees are required to use their personal GitHub accounts to access Drizly projects and data using GitHub, with the company granting those accounts access to its repositories.

## Drizly's Information Security Practices

13. Drizly failed to use reasonable information security practices to protect consumers' personal information. Among other things, Drizly failed to:

    a. 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;

    b. 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);

    c. Impose reasonable data access controls such as: (1) requiring unique and complex passwords (*i.e.*, long passwords not used by the individual for any other online service) 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;

    d. 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;

e. 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

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

## Drizly's Information Security Statements

14. Drizly made explicit representations about its information security practices that led consumers to believe that it used reasonable and appropriate information security practices to protect their personal information.

15. For example, Drizly's Privacy Policy in effect from September 1, 2016 until approximately October 1, 2019 included the following statement:

> Security. All information we collect is securely stored within our database, and we use standard, industry-wide, commercially reasonable security practices such as 128-bit encryption, firewalls and SSL (Secure Socket Layers).

(**Exhibit A**, Drizly.com Privacy Policy)

16. Drizly's Privacy Policy in effect after October 1, 2019 contained similar language:

> Security. We use standard security practices such as encryption and firewalls to protect the information we collect from you.

(**Exhibit B**, Drizly.com Privacy Policy)

## 2020 Breach of Personal Information

17. Drizly's failures, as described in Paragraph 13, led to a breach in or around July 2020 of its production environment, and the exfiltration of the personal information of 2.5 million consumers.

18. In April 2018, Drizly granted a company executive access to its GitHub repositories so that he could participate in a one-day hackathon (a collaborative programming event). Following the event, Drizly failed to monitor and terminate the executive's access, even though such access was no longer needed. The lack of need was underscored by the fact that the executive never accessed the repositories after the hackathon and started employment for a different Drizly subsidiary at the beginning of 2020.

19. Drizly failed to require unique and complex passwords or multifactor authentication for personal GitHub accounts that it granted access to its repositories, nor did it leverage Single Sign On for the GitHub organization. Consequently, the executive's GitHub account used a seven-character alphanumeric password that he had used for other personal accounts and did not use multifactor authentication although it was available.

20. In early July 2020, a malicious actor accessed the executive's GitHub account by reusing credentials from an unrelated breach. The malicious actor then used the executive's GitHub account to access one of Drizly's GitHub repositories containing source code, which it could use to find vulnerabilities in Drizly's software. It was also able to access, in those same repositories, AWS and database credentials.

21. Drizly employees stored these credentials in the company's GitHub repository even though GitHub security guidance and numerous publicly-reported security incidents since 2013 have highlighted the dangers of storing passwords and other access keys in GitHub repositories. For example, the Commission's 2018 Complaint against Uber Technologies Inc. specifically publicized and described credential reuse, lack of multifactor authentication, and insecure AWS credentials exposed through GitHub repository code as failures contributing to the breach and exposure of consumers' personal information.

22. The intruder used the compromised credentials from Drizly's GitHub repositories to modify the company's AWS security settings. This modification provided the intruder unfettered access to Drizly's production environment, including databases containing millions of records of user information. The intruder proceeded to exfiltrate Drizly's User Table, comprising more than 2.5 million records.

23. Drizly did not itself detect the breach of its production environment or discover the exfiltration of the personal information of nearly 2.5 million consumers. Drizly only learned of the breach from media and social media reports describing its customers' accounts for sale on dark web forums.

24. The GitHub compromise and breach of Drizly's production environment was not the company's first security incident involving GitHub. In 2018, another Drizly employee posted Drizly AWS credentials to their individual public (personal) GitHub repository. The employee was unable to delete the GitHub posting or rotate the AWS credentials prior to the public exploitation of the credentials; as a result, Drizly's AWS servers were used to mine cryptocurrency until Drizly learned of the exploitation and changed the credentials. Following this incident, Respondents were on notice of the potential dangers of exposing AWS credentials and should have taken appropriate steps to improve GitHub security, including implementation of policies, procedures, and technical measures to address the security practices of employees with access to Drizly's organizational GitHub repositories.

25. Drizly's own post-breach analyses concluded the company's lack of security preparedness, including failures to operate a formal security program or practice basic security hygiene, was exposed as a result of a data breach.

## Consumer Injury

26. Respondents' failures to provide reasonable security for consumers' personal information have caused or are likely to cause substantial injury to consumers.

27. Consumers have suffered or are likely to suffer substantial injury in the form of increased exposure to fraud and identity theft, leading to monetary loss and time spent remedying

the problem. Personal information exfiltrated from Drizly's databases was offered for sale on two different, publicly-accessible dark web forums, including raidforums.com, a website where criminals post and offer for sale information from compromised databases. Malicious actors combine such information to perpetrate fraud (for example, by opening fraudulent lines of credit) or obtain additional personal information by impersonating companies with whom the target has previously transacted. The opening of fraudulent accounts will cause consumers financial harm in the form of denied transactions due to damaged credit reflected in consumer reports, and time lost in trying to correct those reports. Moreover, as a result of Respondents' failures to secure consumers' personal information, including in many cases their physical addresses, this information is now in the possession of criminals. Consumers are harmed when criminals know and sell their personal information.

28. These harms were not reasonably avoidable by consumers, as consumers had no way of independently knowing about Respondents' security failures (described in Paragraph 13 above).

29. Respondents could have prevented or mitigated the failures described in Paragraph 13 through well known, readily available, and relatively low-cost measures. For example, Drizly could have required regular review of access permissions, multifactor authentication for all employees with access to code repositories, or scanning of code repositories for unsecured credentials. Any of these measures would likely have prevented the July 2020 breach.

## Violations of the FTC Act

30. The acts and practices of Respondents, as alleged in this Complaint, constitute unfair and/or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

## Count I – Drizly's Unfair Information Security Practices

31. As alleged in Paragraphs 13 to 29, Respondents' failure to employ reasonable security measures to protect consumers' personal information 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. This practice was, and is, an unfair act or practice.

## Count II – Drizly's Deceptive Security Statements

32. Through the means described in Paragraphs 14 to 16, Respondents have represented, directly or indirectly, expressly or by implication, that Drizly used appropriate safeguards to protect consumers' personal information.

33. In truth and in fact, as described in Paragraph 13, Respondents did not maintain appropriate safeguards to protect consumers' personal information. Therefore, the representations set forth in Paragraph 32 are false or misleading.

THEREFORE, the Federal Trade Commission this 9th day of January, 2023, has issued this complaint against Respondents.

By the Commission.

April J. Tabor
Secretary

SEAL:

# Exhibit A

# Drizly.com Privacy Policy, September 1, 2016

Security. All information we collect is securely stored within our database, and we use standard, industry-wide, commercially reasonable security practices such as 128-bit encryption, firewalls and SSL (Secure Socket Layers). However, as effective as encryption technology is, no security system is impenetrable. We cannot guarantee the security of our database, nor can we guarantee that information you supply won't be intercepted while being transmitted to us over the Internet, and any information you transmit to Drizly you do so at your own risk. We recommend that you use unique numbers, letters and special characters in your password and not disclose your password to anyone. If you do share your password or personal information with others, you are responsible for all actions taken in the name of your account. Please review our Terms of Service for additional information. If your password has been compromised for any reason, you should immediately notify Drizly at info@drizly.com and change your password.

# Exhibit B

# Drizly.com Privacy Policy, October 1, 2019

Security. We use standard security practices such as encryption and firewalls to protect the information we collect from you. No security system is perfect, and we do not guarantee the security of your information. You are responsible for all actions taken in the name of your account, so use your discretion when providing information and managing your account. Use unique numbers, letters and special characters in your password and do not disclose it to anyone. Please review our Terms of Service for additional information. If your password is compromised notify us immediately at info@drizly.com and change your password. We may store the information we collect on servers in the United States.

**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

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

| | |
|---|---|
| **In the Matter of**<br><br>**DRIZLY, LLC, a Limited Liability Company,**<br>**and**<br><br>**JAMES CORY RELLAS, individually, and as an officer of DRIZLY, LLC.** | **DECISION AND ORDER**<br><br>**DOCKET NO. C-4780** |

## DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondents named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondents a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondents with violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).

Respondents and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: (1) statements by Respondents that they neither admit nor deny any of the allegations in the draft Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit the facts necessary to establish jurisdiction; and (2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondents have violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further

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. Respondent Drizly, LLC ("Drizly"), a Delaware Limited Liability Company with its principal office or place of business at 501 Boylston Street, Boston, MA 02216.

    b. Respondent James Cory Rellas, an officer of Corporate Respondent, Drizly, LLC. Individually or in concert with others, he formulates, directs, or controls the policies, acts, or practices of Drizly, LLC. His principal office or place of business is the same as that of Drizly, LLC.

2. The Commission has jurisdiction over the subject matter of this proceeding and over Respondents, and the proceeding is in the public interest.

## ORDER

## Definitions

For purposes of this Order, the following definitions apply:

1. "**Covered Business**" means: (1) Corporate Respondent; and (2) any business that Corporate Respondent controls, directly or indirectly.

2. "**Corporate Respondent**" means Drizly, LLC, and its successors and assigns.

3. "**Covered Incident**" means any incident that results in a Covered Business notifying, pursuant to a statutory or regulatory requirement, any U.S. federal, state, or local government entity that information of or about an individual consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

4. "**Covered Information**" means information from or about an individual consumer, including: (a) a first and last name; (b) a home or physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) a driver's license or other government-issued identification number; (f) date of birth; (g) Geolocation information sufficient to identify street name and name of a city or town; (h) credit or debit card information (including a partial credit or debit card number); (i) User identifier, or other persistent identifier that can be used to recognize a User over time and across different devices, websites, or online services; or (j) User account credentials, such as a login name and password (whether plain text, encrypted, hashed, and/or salted).

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 otherwise protects the privacy, security, availability, confidentiality, or integrity of any Covered Information; or

C. The extent of any Covered Incident or unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of Covered Information.

### II. Mandated Deletion and Data Minimization

**IT IS FURTHER ORDERED** that Corporate Respondent must:

A. Within 60 days after the issuance date of this Order, Delete or destroy all Covered Information that is not being used or retained in connection with providing products or services to Corporate Respondent's customers, and provide a written statement to the Commission, pursuant to the Provision entitled Compliance Report and Notices, confirming that all such data has been Deleted or destroyed specifically enumerating which types of information were Deleted or destroyed; and

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 collected; (2) the specific business needs for retaining each type of Covered Information; and (3) a set timeframe for Deletion of each type of Covered Information that precludes indefinite retention of any Covered Information; and

B. Within 60 days after the issuance date of this Order, Corporate Respondent shall provide a written statement to the Commission, pursuant to the Provision entitled Compliance Report and Notices, describing the retention schedule for Covered Information made publicly available on its website(s) or app(s); and

C. Prior to collecting any new type of information related to consumers that was not being collected as of the issuance date of this Order, and is not described in retention schedules published in accordance with sub-Provision A of this Provision entitled Data Retention Limits, Corporate Respondent must update its retention schedule setting forth: (1) the purpose or purposes for which the new information is collected; (2) the specific business needs for retaining the new information; and (3) a set timeframe for Deletion of the new information that precludes indefinite retention.

## IV. Mandated Information Security Program for Covered Businesses

**IT IS FURTHER ORDERED** that Corporate Respondent and any business that Corporate Respondent controls, directly or indirectly, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must each, within 60 days of the effective date of this Order, establish and implement, and thereafter maintain, a comprehensive information security program ("Information Security Program") that protects the security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, each Covered Business must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Information Security Program;

B. Provide the written Information Security Program and any evaluations thereof or updates thereto to any Covered Business' board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of the Covered Business responsible for the business' Information Security Program at least once every 12 months and promptly (not to exceed 30 days) after a Covered Incident;

C. Designate a qualified employee or employees to coordinate and be responsible for the Information Security Program;

D. Assess and document, at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Covered Information that could result in the (1) unauthorized collection, maintenance, alteration, use, disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information;

E. Design, implement, maintain, and document safeguards that control for the internal and external risks Covered Businesses identify to the security, confidentiality, or integrity of Covered Information identified in response to sub-Provision D of the Provision entitled Mandated Information Security Program for Covered Businesses. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information. Such safeguards must also include:

    1. A written information security policy and accompanying written standards and procedures that describe, at a minimum: (a) how each Covered Business implements each of the safeguards identified in this sub-Provision; and (b) how each Covered Business assesses and enforces compliance with these safeguards and any other controls it identifies in the policy and accompanying standards and procedures;

    2. Standards, procedures, and policy provisions mandating security education that address internal or external risks each Covered Business identifies under sub-Provision D of this Provision, and that includes, at a minimum: (a) training for each Covered Business' employees about each Covered Business' security policy, standards, and procedures, including the requirements of this Order and the process for submitting complaints and concerns, to be conducted when an employee begins employment or takes on a new role, and on at least an annual basis thereafter; and (b) training in secure software development principles, including secure engineering and defensive programming concepts, for developers, engineers, system administrators, and other employees that design,

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;

10. Technical measures to safeguard against unauthorized access, including: (a) an intrusion prevention or detection system; (b) file integrity monitoring tools; (c) data loss prevention tools; (d) properly configured firewalls; and (e) properly configured physical or logical segmentation of networks, systems, and databases;

11. Technical measures, standards, procedures, and policy provisions to assess the risk posed by source code to Covered Information stored on any Covered Business' network or other assets, including, at least once every 12 months and promptly (not to exceed 30 days) after a Covered Incident involving a vulnerability related to Respondent's source code: (a) software code review; and (b) penetration testing of each Covered Business' software; and

12. Technical measures, procedures, and policy provisions to systematically inventory Covered Information in each Covered Business' control and Delete Covered Information that is no longer necessary;

F. Assess, at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Covered Information, and modify the Information Security Program based on the results;

G. Test and monitor the effectiveness of the safeguards in place at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, and modify the Information Security Program based on the results. Such testing and monitoring must include: (1) vulnerability testing of each Covered Business' network and applications once every 4 months and promptly (not to exceed 30 days) after a Covered Incident; and (2) penetration testing of each Covered Business' network(s) and applications at least once every 12 months and promptly (not to exceed 30 days) after a Covered Incident;

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from each Covered Business, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Covered Information; and

I. Evaluate and adjust the Information Security Program in light of any changes to a Covered Business' operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in sub-Provision D of the Provision entitled Mandated Information Security Program for Covered Businesses, or any other circumstances that a Covered Business or its officers, agents, or employees know or have reason to know may have an impact on the effectiveness of the Information Security Program or any of its individual safeguards. At a minimum, each Covered Business must evaluate the Information Security Program at least once every 12 months and modify the Information Security Program based on the results.

## V. Third Party Information Security Assessments for Covered Businesses

**IT IS FURTHER ORDERED** that, in connection with compliance with the Provision entitled Mandated Information Security Program for Covered Businesses, Corporate Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Information Security Program; and (3) retains all documents relevant to each Assessment for 5 years after completion of such Assessment and will provide such documents to the Commission within 10 days of receipt of a written request from a representative of the Commission. No documents may be withheld by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim.

B. For each Assessment, Corporate Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in their sole discretion.

C. The reporting period for the Assessments must cover: (1) the first 180 days after the Mandated Information Security Program for Covered Businesses required by Provision IV of this Order has been put in place for the initial Assessment; and (2) each two-year period thereafter for 20 years after issuance of the Order for the biennial Assessments.

D. Each Assessment must, for the entire assessment period:

    1. Determine whether Corporate Respondent has implemented and maintained the Information Security Program required by the Provision entitled Mandated Information Security Program for Covered Businesses;

    2. Assess the effectiveness of Corporate Respondent's implementation and maintenance of sub-Provisions A-I of the Provision entitled Mandated Information Security Program for Covered Businesses;

    3. Identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program;

    4. Address the status of gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and

    5. Identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise

of the business's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Corporate Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Corporate Respondent's management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent Corporate Respondent revises, updates, or adds one or more safeguards required under the Provision entitled Mandated Information Security Program for Covered Businesses in the middle of an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

E. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Corporate Respondent must submit an unredacted copy of the initial Assessment and a proposed redacted copy suitable for public disclosure of the initial Assessment to the Commission within 10 days after the Assessment has been completed 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." Corporate Respondent must retain an unredacted copy of each subsequent biennial Assessment as well as a proposed redacted copy of each subsequent biennial Assessment suitable for public disclosure until the Order is terminated and must provide each such Assessment to the Associate Director for Enforcement within ten (10) days of request. The initial Assessment and any subsequent biennial Assessment provided to the Commission must be marked, in the upper right-hand corner of each page, with the words "DPIP Assessment" in red lettering.

## VI. Cooperation with Third-Party Information Security Assessor

**IT IS FURTHER ORDERED** that Respondents, whether acting directly or indirectly, in connection with any Assessment required by the Provision entitled Third Party Information Security Assessments for Covered Businesses must:

A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;

B. Provide or otherwise make available to the Assessor information about Corporate Respondent's networks and all of Corporate Respondent's information technology assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the networks and information technology assets deemed in scope; and

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 for information security, must within 180 days ensure that the business has established and implemented, and thereafter maintains, a comprehensive information security program ("Business ISP") that protects the security, confidentiality, and integrity of Covered Information. To satisfy this requirement, Individual Respondent must ensure that each Relevant Business, at a minimum:

A. Documents in writing the content, implementation, and maintenance of the Business ISP;

B. Provides the written Business ISP and any evaluations thereof or updates thereto to any Relevant Business's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of the Relevant Business responsible for the Business ISP at least once every 12 months;

C. Designates a qualified employee or employees to coordinate and be responsible for the Business ISP;

D. Assesses and documents, at least once every 12 months, internal and external risks to the security, confidentiality, or integrity of Covered Information that could result in the (1) unauthorized collection, maintenance, alteration, use, disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, destruction, or other compromise of such information;

E. Designs, implements, maintains, and documents safeguards that control for the internal and external risks to the security, confidentiality, or integrity of Covered Information identified in response to sub-Provision D of this provision entitled Mandated Information Security Program for Certain Businesses of the Individual Respondent. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information;

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 must include: (1) vulnerability testing of the Relevant Business's network and applications once every 4 months; and (2) penetration testing of the Relevant Business's network(s) and applications at least once every 12 months;

H. Selects and retains service providers capable of safeguarding Covered Information they access through or receive from the Relevant Business, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Covered Information; and

I. Evaluates and adjusts the Business ISP in light of any changes to the Relevant Business's operations or business arrangements, new or more efficient technological or operational methods to control for the risks identified in sub-Provision D of this provision entitled Mandated Information Security Program for Certain Businesses of the Individual Respondent, or any other circumstances that Individual Respondent or the Relevant Business know or have reason to know may have an impact on the effectiveness of the Business ISP or any of its individual safeguards. At a minimum, each Relevant Business must evaluate the Business ISP at least once every 12 months and modify the Business ISP based on the results.

## VIII. Annual Certification

**IT IS FURTHER ORDERED** that Corporate Respondent must:

A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from Corporate Respondent's Chief Executive Officer, James Cory Rellas, or if Mr. Rellas no longer serves as Corporate Respondent's Chief Executive Officer, President, or such other officer (regardless of title) that is designated in Corporate Respondent's Bylaws or resolution of the Board of Directors as having the duties of the principal executive officer of Corporate Respondent, then a senior corporate manager, or, if no such senior corporate manager exists, a senior officer responsible for Corporate Respondent's Information Security Program that: (1) each Covered Business has established, implemented, and maintained the requirements of this Order; (2) each Covered Business is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents that Corporate Respondent verified or confirmed during the certified period. The certification must be based on the personal knowledge of Mr. Rellas, the senior corporate manager, senior officer, or subject matter experts upon whom Mr. Rellas, the senior corporate manager, or senior officer reasonably relies in making the certification.

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 this Order:

A. Each Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

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) identify all of that Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales, and the involvement of any other Respondent (which Individual Respondent must describe if they know or should know due to their own involvement); (d) describe in detail whether and how that Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes the Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

2. Additionally, Individual Respondent must: (a) identify all their telephone numbers and all their physical, postal, email and Internet addresses, including all residences; (b) identify all their business activities, including any business for which such Respondent performs services whether as an employee or otherwise and any entity in which such Respondent has any ownership interest; (c) describe in detail such Respondent's involvement in each such business activity, including

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 compliance notice, sworn under penalty of perjury, within 14 days of any change in the following:

1. Each Respondent must submit notice of any change in: (a) any designated point of contact; or (b) the structure of Corporate Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

2. Additionally, Individual Respondent must submit notice of any change in: (a) name, including alias or fictitious name, or residence address; or (b) title or role in any business activity, including (i) any business for which Respondent performs services whether as an employee or otherwise and (ii) any entity in which Respondent has any ownership interest and over which Respondent has direct or indirect control. For each such business, also identify its name, physical address, any Internet address, and whether or not it is a Relevant Business.

C. Each Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions 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.

## XII. Recordkeeping

**IT IS FURTHER ORDERED** that Respondents must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years, unless otherwise specified below. Specifically, Corporate Respondent and Individual Respondent for any business that such Respondent, individually or collectively with any other Respondents, is a

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 integrity of Covered Information;

F. For 5 years after the date of preparation of each Assessment required by this Order, all materials and evidence that the Assessor considered, reviewed, relied upon or examined to prepare the Assessment, whether prepared by or on behalf of Respondents, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondents' compliance with related Provisions of this Order, for the compliance period covered by such Assessment;

G. For 5 years from the date received, copies of all subpoenas and other communications with law enforcement, if such communications relate to Respondents' compliance with this Order;

H. For 5 years from the date created or received, all records, whether prepared by or on behalf of Respondents, that tend to show any lack of compliance by Respondents with this Order; and

I. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

## XIII. Compliance Monitoring

**IT IS FURTHER ORDERED** that, for the purpose of monitoring Respondents'

compliance with this Order:

A. Within 10 days of receipt of a written request from a representative of the Commission, Respondents must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondents. Respondents must permit representatives of the Commission to interview anyone affiliated with Respondents who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondents or any individual or entity affiliated with Respondents, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

## XIV. Order Effective Dates

**IT IS FURTHER ORDERED** that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance, (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 20 years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

*Provided, further,* that if such complaint is dismissed or a federal court rules that the Respondents did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED: January 9, 2023