)E: 6750-01-P

FEDERAL TRADE COMMISSION

[File No. 202 3185]

Drizly, LLC; Analysis of Proposed Consent Order to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed consent agreement; request for comment.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis of Proposed Consent Order to Aid Public Comment describes both the allegations in the draft complaint and the terms of the consent order—embodied in the consent agreement—that would settle these allegations.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Interested parties may file comments online or on paper by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Please write "Drizly, LLC; File No. 202 3185" on your comment and file your comment online at *https://www.regulations.gov* by following the instructions on the web-based form. If you prefer to file your comment on paper, please mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Jamie Hine (202-326-2188) or Elizabeth Averill (202-326-2993), Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule § 2.34, 16 CFR § 2.34, notice is hereby

given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of 30 days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained at *https://www.ftc.gov/news-events/commission-actions*.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. Write "Drizly, LLC; File No. 202 3185" on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the *https://www.regulations.gov* website.

Because of heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comments online through the *https://www.regulations.gov* website.

If you prefer to file your comment on paper, write "Drizly, LLC; File No. 202 3185" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex D), Washington, DC 20580.

Because your comment will be placed on the publicly accessible website at *https://www.regulations.gov*, you are solely responsible for making sure your comment does not include any sensitive or confidential information. In particular, your comment should not include sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure your

comment does not include sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential"—as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule § 4.10(a)(2), 16 CFR 4.10(a)(2)—including competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule § 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule § 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the *https://www.regulations.gov* website—as legally required by FTC Rule § 4.9(b)—we cannot redact or remove your comment from that website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule § 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at *http://www.ftc.gov* to read this document and the news release describing the proposed settlement. The FTC Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *https://www.ftc.gov/site-information/privacy-policy*.

Analysis of Proposed Consent Order to Aid Public Comment

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 30 days for receipt of comments from interested persons. Comments received during this period will become part of the public record. After 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 failed to 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. It also

alleges Respondent's failures caused or are 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 Drizly made false statements on its corporate website and in its mobile apps about its information security practices. Specifically, Corporate Respondent misrepresented to consumers that the information it collects from them is securely stored and protected by commercially reasonable security practices. The complaint alleges 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 Drizly 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.

Drizly 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.

By direction of the Commission, Commissioner Wilson dissenting in part.

April J. Tabor,

Secretary.

Statement of Chair Lina M. Khan Joined by Commissioner Alvaro M. Bedoya

Today the Commission announced a settlement with the alcohol delivery platform Drizly, LLC, and its CEO, James Cory Rellas, over the company's alleged failure to implement reasonable security policies. According to the complaint, this failure led to several data breaches that exposed the personal information of 2.5 million consumers. Drizly, a wholly owned subsidiary of Uber, collects and stores a vast amount of user data, including names, physical addresses, geolocation, and alcohol order history. It also stores information about consumers that it purchases from third parties.

The Commission's complaint alleges that in 2018, Rellas and Drizly were alerted to security weaknesses that put its stockpile of consumer data at risk, yet they did not address the problem. According to the complaint, the company neglected to implement basic best practices, such as developing a written data security policy or hiring a qualified employee responsible for data security. Then, in 2020, a hacker was able to access a

massive trove of customer data by using login credentials reused by an executive across personal accounts. During this period, Drizly also allegedly made multiple misrepresentations about its data security practices in the privacy policy on its corporate website.

The Commission's proposed order imposes several important conditions to prevent similar failures in the future. It prohibits Drizly from collecting or storing consumer data that is not necessary for pre-specified business purposes. Drizly must also implement a comprehensive security program that features the latest multifactor authentication requirements outlined in recent orders and prevents storage of unsecured credentials on its network or in any cloud-based service. In addition, Drizly must create a public retention schedule for such data, including timeframes for eventual deletion of stored data.

Notably, the order applies personally to Rellas, who presided over Drizly's lax data security practices as CEO. In the modern economy, corporate executives sometimes bounce from company to company, notwithstanding blemishes on their track record.[1] Recognizing that reality, the Commission's proposed order will follow Rellas even if he leaves Drizly. Specifically, Rellas will be required to implement an information security program at future companies if he moves to a business collecting consumer information from more than 25,000 individuals, and where he is a majority owner, CEO, or senior officer with information security responsibilities. Our colleague Commissioner Wilson dissents from the portion of the settlement that personally applies to Rellas. She argues that CEOs of large companies must be allowed to decide for themselves whether or not to pay attention to data security. Respectfully, we disagree. Overseeing a big company is not an excuse to subordinate legal duties in favor of other priorities. The FTC has a role to play in making sure a company's legal obligations are weighed in the boardroom. Today's

---

[1] *See, e.g.*, Rani Molla, *Why Does the WeWork Guy Get to Fail Up?,* RECODE (Aug 17, 2022), https://www.vox.com/recode/2022/8/17/23309756/wework-adam-neumann-flow-andreessen-venture-capital.

settlement sends a very clear message: protecting Americans' data is not discretionary. It must be a priority for any chief executive. If anything, it only grows more important as a firm grows.

Today's action will not only correct Drizly's lax data security practices but should also put other market participants on notice. Limiting the baseline collection and retention of data, as we do here, is a critical tool for protecting Americans from the risks of data breaches, and we will continue to explore remedies centered on limiting the data that is collected or retained in the first place.[2] Finally, holding individual executives accountable, as we also do here, can further ensure firms and the officers that run them are better incentivized to meet their legal obligations.[3]

---

[2] *See* Press Release, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (Mar. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover; Press Release, Fed. Trade Comm'n, Press Release, Fed. Trade Comm'n, FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data (Mar. 4, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive; *see also* Statement of Chair Lina M. Khan Regarding the Report to Congress on Privacy and Security (Oct. 1, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597024/statement_of_chair_lina_m_khan_regarding_the_report_to_congress_on_privacy_and_security_-_final.pdf; Remarks of Chair Lina M. Khan As Prepared for Delivery, IAPP Global Privacy Summit 2022 (Apr. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf; *see generally* Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51,273 (Aug. 22, 2022).

[3] *See* Press Release, Fed. Trade Comm'n, FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data (Sept. 1, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data.

Statement of Commissioner Rebecca Kelly Slaughter

The kinds of lax and unreasonable data security practices the Commission has alleged in this settlement with Drizly[1] have caused immense and often incalculable harm to consumers. As the complaint recounts, Drizly's carelessness with customer information led to an intruder gaining access to its systems and downloading the personal information of 2.5 million people.

This order is commendable and marks a meaningful step forward in our data security enforcement. Naming Drizly's CEO, James Corey Rellas, who oversaw these practices, helps ensure that corporate leadership must take seriously their obligation to safeguard customer information. Mechanisms like the proposed data retention schedule are also an excellent approach to provide accountability for data use and misuse. Ensuring that Drizly only collects information necessary to effectuate its published business needs should exert a disciplining influence on its collection of consumer information. The retention schedule also provides a clear hook for future FTC enforcement actions should Drizly not follow its strict requirements under this proposed order.

Going forward, I believe the law would support us doing more to safeguard Americans' data, including requiring substantive limits on appropriate collection and use. While the disclosure requirements in this order have value, disclosure alone is not enough. We know that endless terms-of-service and other disclosures have not improved customer understanding, facilitated meaningful choice, or protected data from security breaches. But hackers cannot steal data that companies did not collect in the first place; requirements that limit what data can be collected, used, and retained could meaningfully foil and deter data security breaches.

---

[1] Drizly is now a wholly owned subsidiary of Uber which reached a settlement with the FTC over its allegedly lax data security practices in 2018. I worry greatly about this matryoshka doll of companies with a spotty track record of protecting consumer data.

There are many ways to approach data collection guardrails. As the FTC further develops a minimization framework, one framework I hope we consider is centering a consumer's reasonable expectation that there should be limits on the collection and use of their information based on the service they've actually requested. I believe the agency is in a better position to effectuate this expectation than it is to anticipate, understand, and police every claim of reasonable business necessity. A consumer centered data minimization standard could work hand-in-hand with the kinds of disclosures and effective data security practices in this proposed order to protect Americans from the ongoing epidemic of data breaches, which are greatly exacerbated by overcollection of consumer information.

I am grateful to the staff for their hard work on this strong order. I look forward to seeing how our work continues to evolve in the pursuit of protecting Americans' data and ensuring our confidence in the practices of the businesses with which we all transact.

Concurring and Dissenting Statement of Commissioner Christine S. Wilson

Today the Commission announces a complaint and settlement resolving allegations that Drizly, LLC and its CEO, James Cory Rellas, violated Section 5 of the FTC Act. The complaint asserts that Drizly made false statements on its website and in its mobile apps about its information security practices. The Commission also alleges that Drizly engaged in several unreasonable data security practices that led to multiple security breaches, including a hacker's unauthorized download of personal information about 2.5 million consumers.

The FTC has long provided clear guidance to the business community about the fundamentals of sound data security.[1] But, as the complaint details, Drizly failed to

[1] Fed. Trade Comm'n, *Start with Security: A Guide for Business* (Jun. 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business; Press Release, Fed. Trade Comm'n, Stick with Security: FTC to Provide Additional Insights on Reasonable Data Security Practices (July 21, 2017), https://www.ftc.gov/news-events/press-releases/2017/07/sticksecurity-ftc-provide-additional-insights-reasonable-data.

require unique and complex passwords or multifactor authentication to access source code or databases; failed to terminate employee or contractor access to data once they no longer needed such access; failed to monitor for unauthorized attempts to transfer or exfiltrate consumers' personal information outside company networks; and engaged in other security shortcomings. Notably, simple, readily available, low-cost measures could have addressed Drizly's security shortcomings. I support the complaint against the company and the order provisions that require Drizly to implement numerous data security practices to address the company's missing security safeguards.[2] In particular, my Democratic colleagues and I agree that data minimization plays an important role in a healthy data security program. As Commissioner Slaughter notes in her concurring statement, "hackers cannot steal data that companies did not collect in the first place."

While I support the complaint against the corporate defendant, I do not support holding the individual defendant, Rellas, liable. To seek injunctive relief with respect to a CEO or other principal, the Commission must show only that the individual "participated directly in the deceptive practices *or* had authority to control those practices."[3] Authority to control does not require the FTC to show a "specific link from [the individual] to the particular deceptive [acts] and instead looks at whether [the individual] had authority to control the corporate entity's practices."[4] This broad standard effectively could enable the

---

[2] While I support the settlement against Drizly, I continue to question whether data security orders should remain in effect for 20 years. It is not realistic for the Commission to expect that injunctive relief with respect to this dynamic and rapidly evolving issue will remain relevant and beneficial to consumers for 20 years. *See* Concurring Statement of Commissioner Christine S. Wilson, *In the Matter of* InfoTrax Systems, L.C. and Mark Rawlins, File No. 1623130 (Nov. 19, 2020), https://www.ftc.gov/system/files/documents/public_statements/1553676/162_3130_infotrax_concurring_statement_cw_11-12-2019.pdf.

[3] *FTC v. Ross*, 743 F.3d 886, 892-93 (4th Cir. 2014) (adopting the test for individual liability used by other federal appellate courts, including the First, Seventh, Ninth, Tenth, and Eleventh Circuits). The Commission also can establish liability for monetary relief by showing the defendant "had actual knowledge of the deceptive conduct, was recklessly indifferent to its deceptiveness, or had an awareness of a high probability of deceptiveness and intentionally avoided learning the truth." *Id*.

[4] *Id*. at 893.

Commission to hold individually liable the CEOs of most companies against which we initiate enforcement action.

The Commission traditionally has exercised its prosecutorial discretion and assessed a variety of factors when deciding whether to name a CEO or principal, including consideration of whether individual liability is necessary to obtain effective relief, and the level of the individual's knowledge and participation in the alleged illegal conduct.[5]

The order against Drizly requires the company to implement extensive data security safeguards regardless of whether Rellas is at the helm of the organization. Naming Rellas does not change the injunctive obligations placed on the company to ensure that customers' personal information is protected going forward. Moreover, the case against Drizly makes clear that the FTC expects technology start-ups to start with security and establish reasonable data security practices that grow with the company.

As for knowledge and participation, the number of issues crossing a CEO's desk on any given day is substantial. In most large companies, I would expect CEOs to have little to no involvement with, and no direct knowledge of, practices that are the subject of an FTC investigation. Here, we do not allege that Rellas oversaw day-to-day operations of the company's data security practices, had any data security expertise, or was responsible for decisions about data security policies, procedures, or programs.[6] Instead, we allege that Rellas did not appropriately prioritize hiring a senior executive responsible for privacy and

---

[5] Many FTC cases involve fraudulent or deceptive conduct by small, closely held companies that essentially serve as the alter egos of their principal or CEO. I support naming the CEO in such a case because the individual defendant is necessary to obtain effective relief and/or to prevent the fraudster from opening and shuttering companies to stay one step ahead of law enforcement. *See* Concurring Statement of Commissioner Christine S. Wilson Regarding FTC v. Progressive Leasing, LLC, File No. 1823127 (April 20, 2020), https://www.ftc.gov/system/files/documents/public_statements/1571921/182_3127_prog_leasing_-_statement_of_commissioner_christine_s_wilson_0.pdf.

[6] *Cf* Complaint, *In re InfoTrax Systems, L.C., a limited liability company, and Mark Rawlins*, Docket No. C-4696 (Dec. 30, 2019) (alleging Rawlins spent eighteen years at a software company, studied computer science in college, "reviewed and approved InfoTrax's information technology security policies, was involved in discussions with clients about data security regularly, and was involved in the company's long-term data security strategy."), https://www.ftc.gov/system/files/documents/cases/c-4696_162_3130_infotrax_complaint_clean.pdf.

data security. Our complaint notes that he hired other members of the c-suite but not a Chief Technology Officer or Chief Information Security Officer. And for Rellas' failure to prioritize information security over other business obligations, the order imposes on Rellas significant compliance obligations even if he leaves Drizly.[7]

By naming Rellas, the Commission has not put the market on notice that the FTC will use its resources to target lax data security practices. Instead, it has signaled that the agency will substitute its own judgement about corporate priorities and governance decisions for those of companies.[8] There is no doubt that robust data security is important. Having a federal data security law would signal to companies, executives, and boards of directors the importance of implementing and maintaining data security programs that address potential risks, taking into account the size of the business and the nature of the data at issue. But CEOs have hundreds of issues and numerous regulatory obligations to navigate. Companies, not federal regulators, are better positioned to evaluate what risks require the regular attention of a CEO. And when companies err in making those assessments, the government will hold them accountable.

Accordingly, I dissent from the inclusion of the individual defendant in the complaint and settlement in this matter.

[FR Doc. 2022-23669 Filed: 10/31/2022 8:45 am; Publication Date: 11/1/2022]

---

[7] The Order binds Rellas to implement an information security program at any future company in which he is a majority owner, CEO, or senior officer with information security responsibilities, where that company collects personal information from at least 25,000 individuals. The Order does not address scenarios in which Boards of Directors, other owners, or higher-ranking executives make it impossible for Rellas to fulfill his obligations.

[8] Then-Commissioner Phillips and I raised similar concerns in our dissents to the FTC's regulatory reviews of the Safeguards Rule. *See* Joint Statement of Commissioners Noah Joshua Phillips and Christine S. Wilson, In the Matter of the Final Rule amending the Gramm-Leach-Bliley Act's Safeguards Rule, File No. P145407 (Oct. 27, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597994/joint_statement_of_commissioners_phillips_and_wilson_in_the_matter_of_regulatory_review_of_the_1.pdf; Dissenting Statement of Commissioner Noah Joshua Phillips and Commissioner Christine S. Wilson, Regulatory Review of Safeguards Rule, File No. P145407 (Mar. 5, 2019), https://www.ftc.gov/system/files/documents/public_statements/1466705/reg_review_of_safeguards_rule_cmr_phillips_wilson_dissent.pdf.