

Complaint

IN THE MATTER OF

ASCENSION DATA & ANALYTICS, LLC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF THE GRAMM-LEACH-BLILEY
ACT.

Docket No. C-4758; File No. 191 0153
Complaint, December 22, 2021 – Decision, December 22, 2021

This consent order addresses Ascension Data & Analytics' violation of the GLB Act's Safeguards Rule through the failure to maintain a comprehensive information security program to protect customer information in their control. The complaint alleges that Ascension Data & Analytics' stored sensitive personal information from mortgage documents in plain text on a cloud-based server without any protections to block unauthorized access. Under the order Respondent must establish and implement comprehensive data security protections and oversight of third-party providers to ensure compliance with those safeguards.

Participants

For the *Commission*: Jarad Brown and Miles Plant.

For the *Respondent*: Claudia McCarron and Kathleen Laubenstein [Mullen Coughlin LLC].

COMPLAINT

The Federal Trade Commission, having reason to believe that Ascension Data & Analytics, LLC, a limited liability company, has violated the provisions of the Commission's Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Title I of the Gramm-Leach-Bliley ("GLB") Act, 15 U.S.C. § 6801 *et seq.*; and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Ascension Data & Analytics, LLC ("Ascension" or "Respondent") is a Delaware limited liability company with its principal place of business at 701 Highlander Boulevard, Suite 510, Arlington, Texas 76015.
2. The acts and practices of Respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS ACTIVITIES

3. Respondent is an analytics company that provides data, analytics, and system-based technology services and products to other companies in its corporate family in connection with mortgages. Respondent's many services include systems development, such as the creation of document management systems, automation of data-driven decision-making, and case management task scheduling; creating valuation models and comparative market analyses; and

Complaint

various due diligence reviews or analyses, such as title searches, analyses of foreclosure dockets, and risk analyses related to the foregoing.

4. In or around 2017, Respondent contracted to provide the following services for a related company in connection with due diligence for residential mortgages: (a) building and maintaining a document management system for use in storing, indexing, tracking, organizing, and displaying mortgage documents; (b) valuation review services, which included creating automated valuation models and conducting comparative market analyses; (c) reviewing and analyzing loan servicing comments; (d) compliance reviews related to loan originations; and (e) collateral reviews of imaged documents.

5. Respondent's work for the related company included hiring an unaffiliated company to process the mortgage documents of borrowers relating to approximately 37,000 mortgages. These documents included mortgage applications and various associated documents, such as tax returns, that contained information about 60,593 consumers. The types of personal information in the documents included names, dates of birth, Social Security numbers, loan information, credit and debit account numbers, drivers' license numbers, credit files, or other personal and financial information of borrowers, as well as of family members and others whose information was included in the mortgage applications.

BREACH OF CUSTOMER INFORMATION

6. In February 2017, Respondent contracted with an unaffiliated company, PairPrep, Inc., doing business as OpticsML ("OpticsML"), to conduct Optical Character Recognition ("OCR") scanning on the mortgage documents.

7. Per its own policies, Respondent was required to vet the security measures of OpticsML to ensure it could properly protect the sensitive personal information of consumers. However, Respondent did nothing to assess OpticsML's security measures.

8. Despite never vetting OpticsML's security, Respondent provided it with the aforementioned mortgage documents, which contained the personal information of tens of thousands of consumers, including sensitive financial information.

9. OpticsML stored the contents of the documents on a cloud-based server and in a separate cloud-based storage location. But, in doing so, OpticsML misconfigured both the server and the storage location, leaving the sensitive personal information of tens of thousands of consumers exposed to anyone on the internet for a year, beginning in January 2018. As a result, all that was needed to view or download this personal information was the internet address of the server or the storage location; no password was required.

10. The information sat unprotected until about January 2019, when media reports revealed that this information was publicly exposed online.

Complaint

11. During the year the server and the storage location were unsecured, approximately 52 unauthorized IP addresses accessed them. Most of these IP addresses were associated with computers outside the United States, including addresses from Russia and China.

GRAMM-LEACH-BLILEY ACT SAFEGUARDS RULE

12. Respondent is a financial institution, as that term is defined by Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A), because it is significantly engaged in, among other things, data processing, 12 C.F.R. § 225.28(b)(14); financial and investment advisory services, § 225.28(b)(6); and real estate settlement services, § 225.28(b)(2)(viii). Respondent is subject to the GLB Safeguards Rule, 16 C.F.R. Part 314, because it is a financial institution that handles and maintains nonpublic personal information, as defined by 16 C.F.R. § 313.3(n), that pertains to customers of other financial institutions that provide such information to Respondent.

13. The Safeguards Rule, which implements Section 501(b) of the GLB Act, 15 U.S.C. § 6801(b), was promulgated by the Commission on May 23, 2002, and became effective on May 23, 2003. The Rule requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing, implementing, and maintaining a comprehensive information security program that is written in one or more readily accessible parts, and that contains administrative, technical, and physical safeguards that are appropriate to the financial institution's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issue, including:

- a. Designating one or more employees to coordinate the information security program;
- b. Identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks;
- c. Designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures;
- d. Overseeing service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for customer information, and requiring service providers by contract to implement such safeguards; and
- e. Evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

Complaint

16 C.F.R. §§ 314.3 and 314.4. Violations of the Safeguards Rule are enforced through the FTC Act. 15 U.S.C. § 6805(a)(7).

RESPONDENT FAILED TO OVERSEE SERVICE PROVIDERS

14. Since at least September 2016, Respondent has failed to take reasonable steps to select service providers capable of maintaining appropriate safeguards for the personal information Respondent provided.

15. Since at least July 2016, Respondent maintained a “Third Party Vendor Risk Management” policy describing the due diligence Respondent required for service providers. The policy recommends numerous steps Respondent’s Chief Information Security Officer (CISO) and business managers were to take to evaluate service providers, such as having service providers provide their policies and procedures and fill out an information security questionnaire.

16. Despite its policy, Respondent has not taken any formal steps to evaluate whether service providers could reasonably protect the personal information Respondent had entrusted to them. For example, before Respondent provided documents containing consumers’ sensitive personal information to OpticsML, Respondent did not take any of the steps described in its own policy to evaluate OpticsML’s security capabilities.

17. Since at least September 2016, Respondent has also failed to require service providers by contract to implement appropriate safeguards for personal information that Respondent provided to those service providers. Instead, Respondent’s service provider contracts have only included an agreement that “any nonpublic personal information . . . shall be protected from disclosure with all the provisions of the Gramm-Leach-Bailey [sic] Act,” and not disclosed by either party without prior written consent. But these clauses did not make clear that the service providers, including OpticsML, were responsible for protecting the information in accordance with the GLB’s Safeguards Rule, or that they were even subject to the rule. Respondent’s service provider contracts failed to specify safeguards that service providers must implement, or otherwise require them to take reasonable steps to secure personal information.

18. Indeed, Respondent’s service provider contracts do not satisfy its Third Party Vendor Risk Management policy, which requires Respondent to “contractually require its third party vendors to implement appropriate measures” with respect to customer information.

RESPONDENT FAILED TO ADEQUATELY ASSESS RISK

19. Respondent has also failed to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assess the sufficiency of any safeguards in place to control those risks.

20. Prior to September 2017, Respondent did not conduct adequate risk assessment. During this time, Respondent also did not assess risks related to its service providers, even though

Complaint

its “Third Party Vendor Risk Management” policy required its CISO to “complete a quantitative assessment of risk” for each service provider.

21. In September 2017 and again in October 2018, another company in Respondent’s corporate family arranged for a third-party security company to conduct technology risk assessments of the corporate family, which included some evaluation of Respondent’s security and risks. However, those assessments were limited to a small subset of Respondent’s service providers, and did not assess the security of a long list of other service providers, including OpticsML.

COUNT I
Violation of the GLB Safeguards Rule

22. Respondent is a financial institution, as defined in Section 509(3)(A) of the GLB Act, 15 U.S.C. § 6809(3)(A). Respondent handles and maintains nonpublic personal information, as defined by 16 C.F.R. § 313.3(n), about customers of financial institutions.

23. As set forth in Paragraphs 14-18, Respondent has failed to oversee service providers.

24. As set forth in Paragraphs 19-21, Respondent has failed to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information and failed to assess the sufficiency of any safeguards in place to control those risks.

25. Therefore, the conduct set forth in Paragraphs 23-24 is a violation of the Safeguards Rule, 16 C.F.R. Part 314.

THEREFORE, the Federal Trade Commission this twenty-second day of December 2021, has issued this complaint against Respondent.

By the Commission, Chair Khan not participating and Commissioner Slaughter dissenting.

Decision and Order

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent 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 Respondent with violations of the Federal Trade Commission’s Standards for Safeguarding Customer Information Rule (“Safeguards Rule”), 16 C.F.R. Part 314, issued pursuant to Title I of the Gramm-Leach-Bliley (“GLB”) Act, 15 U.S.C. § 6801 *et seq.*

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: (1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits 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 Respondent has violated the Safeguards Rule and 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 Respondent is Ascension Data & Analytics, LLC, a Delaware limited liability company with its principal place of business at 701 Highlander Boulevard, Suite 510, Arlington, Texas 76015.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER**Definitions**

For purposes of this Order, the following definitions apply:

- A. “Covered Business” means Respondent or any business that Respondent controls.

Decision and Order

- B. “Covered Incident” means any instance in which any United States federal, state, or local law or regulation requires a Covered Business to notify any U.S. federal, state, or local government entity that information from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization.
- C. “Covered Information” means (1) Personally Identifiable Financial Information; and (2) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any Personally Identifiable Financial Information that is not publicly available.
- D. “Personally Identifiable Financial Information” means any information:
 - 1. A consumer provides to obtain a financial product or service;
 - 2. About a consumer resulting from any transaction involving a financial product or service; or
 - 3. A Covered Business otherwise obtains about a consumer in connection with providing a financial product or service to that consumer.
- E. “Respondent” means Ascension Data & Analytics, LLC, a Delaware limited liability company, and its successors and assigns.
- F. “Vendor” means any person or entity that receives, maintains, processes, or otherwise is permitted access to Covered Information from, by, or at the direction of a Covered Business through its provision of services directly to a Covered Business.

Provisions**I. GLB RULE VIOLATIONS**

IT IS ORDERED that Respondent, and 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 violate any provision of the Standards for Safeguarding Consumer Information Rule, 16 C.F.R. Part 314, a copy of which is attached hereto as Exhibit A.

Decision and Order

II. MANDATED DATA SECURITY PROGRAM

IT IS FURTHER ORDERED that each Covered Business must not transfer, sell, share, collect, maintain, or store Covered Information unless it establishes and implements, and thereafter maintains, a comprehensive data security program (“Data Security Program”) that protects the security 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 Data Security Program;
- B. Provide the written program and any evaluations thereof or updates thereto to its board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer responsible for its Data Security Program at least once every twelve (12) months and promptly after a Covered Incident;
- C. Designate a qualified employee or employees to coordinate and be responsible for the Data Security Program;
- D. Assess and document, at least once every twelve (12) months and promptly following a Covered Incident, internal and external risks to the security of Covered Information that could result in the unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of such information. Each such assessment must evaluate risks in each area of relevant operation, including: (1) employee training and management; (2) information systems, such as network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;
- E. Design, implement, maintain, and document safeguards that control the internal and external risks identified in response to sub-Provision II.D. Each safeguard must be based on the volume and sensitivity of the Covered Information at risk, and the likelihood that the risk could be realized and result in the unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of such information. Each Covered Business’s safeguards must also include:
 1. Require each Vendor to:
 - a. Before the Covered Business provides access to Covered Information:
 - i. Provide documentation of its information security policies and practices related to protecting any Covered Information that may be obtained from the Covered Business;

Decision and Order

- ii. Describe in writing how and where the Covered Information will be maintained and what safeguards are in place or will be implemented to protect it;
 - b. Update in writing the information required by sub-Provision II.E.1.a when there is a material change or at least once every twelve (12) months; and
 - c. Implement measures to assess the cybersecurity risk to Covered Information obtained from the Covered Business that is stored on the Vendor's networks, if any, and if any is stored, provide documentation to the Covered Business of the scope of the measures and their results, including, at least once every twelve (12) months and promptly after a Covered Incident: (i) vulnerability scanning; and (ii) penetration testing;
 - 2. Maintain all documentation provided by each Vendor pursuant to sub-Provision II.E.1 for a period of five (5) years from when it was provided; and
 - 3. At least once every twelve (12) months, and promptly following a Covered Incident involving a Vendor, conduct written assessments of each Vendor to determine the continued adequacy of their safeguards to control the internal and external risks to the security of Covered Information. The level of the assessment for each Vendor should be commensurate with the risk it poses to the security of Covered Information.
 - 4. Provided, however, that sub-Provisions II.E.1-3 are not required of any Covered Business for a Vendor that receives, maintains, processes, or otherwise is permitted access to only names and/or property addresses, and to no other Covered Information, from, by, or at the direction of the Covered Business.
- F. Assess, at least once every twelve (12) months and promptly following a Covered Incident, the sufficiency of any safeguards in place to address the risks to the security of Covered Information, and modify the Data Security Program based on the results;
- G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months, and promptly following a Covered Incident, and modify the Data Security Program based on the results;
- H. Select and retain Vendors capable of safeguarding Covered Information they access through or receive from Covered Businesses, and contractually require Vendors to implement and maintain safeguards for Covered Information; and

Decision and Order

- I. Evaluate and adjust the Data Security Program in light of any changes to its operations or business arrangements, a Covered Incident, or any other circumstances that each Covered Business knows or has reason to know may have an impact on the effectiveness of the Data Security Program. At a minimum, each Covered Business must evaluate the Data Security Program at least once every twelve (12) months and modify the Data Security Program based on the results.

III. DATA SECURITY ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Provision II of this Order titled Mandated Data Security Program, Respondent must obtain, for each Covered Business, 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 Data Security Program; and (3) retains all documents relevant to each Assessment for five (5) years after completion of such Assessment and will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld 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, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name and affiliation of the person selected to conduct the Assessment, which the Associate Director shall have the authority to approve in his or her sole discretion.
- C. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment; and (2) each 2-year period thereafter for ten (10) years after issuance of the Order for the biennial Assessments.
- D. Each Assessment must: (1) determine whether each Covered Business has implemented and maintained the Data Security Program required by Provision II of this Order, titled Mandated Data Security Program; (2) assess the effectiveness of each Covered Business’s implementation and maintenance of sub-Provisions II.A-I; (3) identify any gaps or weaknesses in the Data Security Program; and (4) 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 sufficient to justify the Assessor’s findings. No finding of any Assessment shall rely solely on assertions or attestations by a Covered Business’s management. The Assessment must be signed by the Assessor and must

Decision and Order

state that the Assessor conducted an independent review of the Data Security Program, and did not rely solely on assertions or attestations by a Covered Business's management.

- E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Respondent must submit its initial Assessment to the Commission within ten (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 Ascension Data & Analytics, LLC, FTC File No. 1923126." All subsequent biennial Assessments must be retained by Respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

IV. COOPERATION WITH THIRD PARTY INFORMATION SECURITY ASSESSOR

IT IS FURTHER ORDERED that Respondent, whether acting directly or indirectly, in connection with any Assessment required by Provision III of this Order titled Data Security Assessments by a Third Party, must:

- A. 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 the Covered Business has implemented and maintained the Data Security Program required by Provision II of this Order, titled Mandated Data Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions II.A-I; or (3) identification of any gaps or weaknesses in the Data Security Program; and
- B. 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.

V. ANNUAL CERTIFICATION

IT IS FURTHER ORDERED that, in connection with compliance with Provision II of this Order titled Mandated Data Security Program, Respondent must:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of each Covered Business responsible for each Covered Business's Data Security Program that: (1) each Covered Business has established, implemented, and maintained the requirements

Decision and Order

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 any Covered Incident. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom 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 Ascension Data & Analytics, LLC, FTC File No. 1923126.”

VI. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondent, for any Covered Business, within a reasonable time after the date of discovery of a Covered Incident, but in any event no later than ten (10) days after the date the Covered Business first notifies any U.S. federal, state, or local government entity of the Covered Incident, 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 of the Covered Incident, if known;
- C. A description of each type of information that triggered the notification obligation to the U.S. federal, state, or local government entity;
- D. The number of consumers whose information triggered the notification obligation to the U.S. federal, state, or local government entity;
- E. The acts that the 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 required by U.S. federal, state, or local law or regulation and sent by the Covered Business or any of its clients to consumers or to any U.S. federal, state, or local government entity.

Decision and Order

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 Ascension Data & Analytics, LLC, FTC File No. 1923126."

VII. ACKNOWLEDGMENTS OF THE ORDER

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within ten (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 twenty (20) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision VIII of this Order titled Compliance Report and Notices. Delivery must occur within ten (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 Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

VIII. COMPLIANCE REPORTS AND NOTICES

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

- A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which 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 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, and the means of advertising, marketing, and sales; (d) describe in detail whether and how Respondent is in compliance with each Provision of this

Decision and Order

Order, including a discussion of all of the changes 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.

- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (a) any designated point of contact; or (b) the structure of 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.
- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Respondent within fourteen (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 Ascension Data & Analytics, LLC, FTC File No. 1923126.”

IX. RECORDKEEPING

IT IS FURTHER ORDERED that Respondent must create certain records for twenty (20) years after the issuance date of the Order and retain each such record for five (5) years, unless otherwise specified below. Specifically, Respondent must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold;
- 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;

Decision and Order

- C. Copies or records of all consumer complaints and refund requests, whether received directly or indirectly, such as through a third party, and any response;
- D. For five (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 a Covered Business, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Covered Businesses' compliance with related Provisions of this Order, for the compliance period covered by such Assessment;
- E. For five (5) years from the date received, copies of all subpoenas and other communications with law enforcement, if such communications relate to a Covered Business's compliance with this Order;
- F. For five (5) years from the date created or received, all records, whether prepared by or on behalf of a Covered Business, that address compliance by a Covered Business with this Order or lack thereof; and
- G. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

X. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within ten (10) days of receipt of a written request from a representative of the Commission, Respondent 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 Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent 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 Respondent or any individual or entity affiliated with Respondent, 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.

Dissenting Statement

XI. 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 on December 22, 2041, or twenty (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 twenty (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 Respondent 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, Chair Khan not participating, Commissioner Slaughter dissenting.

**DISSENTING STATEMENT OF
COMMISSIONER ROHIT CHOPRA**
December 14, 2020

Summary

- After an egregious data breach involving extremely sensitive financial information, the Commission has struck a settlement that provides no help for victims and does little to deter.

- It appears Ascension Data & Analytics is really just an offshoot of a large investment fund, and the Commission's proposed order fails to bind the appropriate parties.

Dissenting Statement

- To achieve meaningful results, the Commission must reevaluate its enforcement strategy when it comes to safeguarding consumer financial information by working collaboratively with other regulators and applying its unfairness authority in an even-handed manner.

Americans have been burned by the mortgage industry before – not just by slipshod practices that maximize profits at the expense of responsible stewardship, but also by slippery accountability when things go wrong. Regulators got lost in a labyrinth of shell companies and subsidiaries, and too many who profited escaped unscathed, leaving families in ruin.

To achieve the dream of homeownership, Americans typically have to fork over a boatload of personal data to mortgage lenders, like our Social Security numbers, our driver's license numbers, our pay stubs, and more. This is the norm when you borrow to buy a home. The lender then transfers this data onward through the financial system, with banks, servicers, mortgage funds, investment vehicles – and their vendors – all gaining access.

This data, in the wrong hands, is valuable intelligence not only for identity thieves but also for nation states, leading to threats to our financial and national security. That's why federal law ensures that financial institutions have safeguards in place to secure this highly sensitive data.

After a data breach of highly sensitive data from mortgage applications, the FTC launched an investigation into Ascension Data & Analytics. Ascension worked on behalf of its sister companies, such as investment funds to analyze mortgages. Ascension also hired other vendors to help. Even though Ascension was required under the law to guard consumer financial data, in fact, they were using third parties with shoddy security, as alleged in the complaint. Given the breadth and sensitivity of the data compromised in this breach, an individual consumer would probably prefer to be affected by the Equifax breach than this one, if forced to make a choice.

In my view, the Commission's proposed resolution of this investigation suffers from three key flaws: It fails to hold all of the right parties accountable. It fails to charge unfair conduct as unfair. And it fails to redress consumers or deter other firms from engaging in similar misconduct.

Ascension, Rocktop Partners, and Corporate Musical Chairs

Ascension is not really an independent company.¹ It's in the same corporate family as Rocktop Partners,² a multi-billion dollar private equity fund that buys up defective mortgages, such as those with title disputes.³ Ascension's President, Brett Benson, is also Managing Director of Rocktop Partners.⁴ Its office sits on the same floor as Rocktop Partners at 701 Highlander Boulevard in Arlington, Texas.⁵ When the Ascension breach hit the news, it was Rocktop's

¹ My office has endeavored to cite public sources showing a portion of the web of companies involving Ascension, Rocktop, and Reidpin LLC.

² Zack Whittaker, *Millions of bank loan and mortgage documents have leaked online*, TECHCRUNCH (Jan. 23, 2019), <https://techcrunch.com/2019/01/23/financial-files/>.

³ ROCKTOP PARTNERS, <https://rocktoppartners.com> (last visited on Oct. 2, 2020).

⁴ *Id.*

⁵ *Id.*, Compl., *In the Matter of Ascension Data & Analytics, LLC*, Fed. Trade Comm'n File No. 1923126.

Dissenting Statement

General Counsel, Sandy Campbell, who confirmed the key details of the incident.⁶ It is unclear whether Ascension has any clients *other* than Rocktop Partners or others in its corporate family.⁷ This is a common arrangement in finance, since it allows fund managers to profit when they can bill their investors for services.

Further, Rocktop's Managing Director and Chief Financial Officer, Jonathan Bray, is also the sole person ("manager" or "member") listed on the LLC forms for a firm called Reidpin LLC.⁸ Langhorne Reid and Jason Pinson ("**Reid**" and "**Pinson**") are cofounders of Rocktop.⁹ Unsurprisingly, Reidpin LLC is located at the same address as Ascension and Rocktop.¹⁰ It is therefore clear that Ascension is anything but arms-length from Rocktop. Rocktop's corporate structure confirms this conclusion:

Figure 1. 



The FTC has charged Ascension Data & Analytics – but not any other parties in the broader Rocktop family – with violating the Safeguards Rule by failing to police its agents processing personal data. I agree that Ascension violated the law, but I am concerned that the proposed settlement will do little to prevent future failures. In addition, our complaint and the Analysis to Aid Public Comment would be strengthened with critical information about the Rocktop corporate structure.¹¹

The FTC's order binds only one company: Ascension. The company that actually appears to manage more than \$7 billion worth of Americans' mortgages – Rocktop – is not being required to change a single thing about its practices.¹² And while Ascension will be required to clean up its act, nothing is stopping the controllers of Rocktop from creating a "new" analytics firm staffed with exactly the same executives, or even transferring the functions within their corporate family, but without any obligations under the FTC's order. This would be economically rational. The Commission does not cite any sworn testimony or other evidence to show why they believe the controllers of Ascension would act irrationally.

⁶ *Supra* note 2.

⁷ *Id.*

⁸ Reidpin, LLC, Application to Register a Foreign Limited Liability Company (LLC) (Nov. 17, 2020) <https://businesssearch.sos.ca.gov/Document/RetrievePDF?Id=201816410221-24379676>.

⁹ *Supra* note 3.

¹⁰ *Supra* note 8.

¹¹ Commissioner Phillips points to the fact that Rocktop Partners may be a registered investment fund under the securities laws, but does not discuss the other entities within the corporate family and in any related mortgage vehicles that are not.

¹² *Supra* note 3.

Dissenting Statement

Commissioner Phillips argues that this is a concern in cases involving “boiler rooms and other frauds.” I respectfully disagree. When the FTC charged Wyndham in 2012 with lax data security practice, it named not only the parent corporation but also three subsidiaries, alleging that they operated with common control, shared offices, overlapping staff, and as part of a maze of interrelated companies. Defending these charges against dismissal, the Commission argued that “[i]f the Court were to enter an order against only [the subsidiary], Wyndham would be able to transfer responsibility for data security to another Wyndham entity[,]” allowing the company to sidestep its obligations under any order.¹³ The court agreed, specifically rejecting the view that only “shell companies designed to perpetrate fraud” can face charges.¹⁴

The FTC should not be allowing companies to evade accountability through a game of corporate musical chairs. An effective order would bind not only Ascension, but also all of the parties liable under the law. While one of these parties may be outside the jurisdiction of the FTC’s Safeguards Rule, there is no question that they are bound by the FTC Act’s prohibition on unfair practices.

Unfair Conduct is Unlawful, Regardless of Size

The FTC has declined to include a charge of violating the FTC’s prohibition on unfair practices. This represents a departure from previous cases involving similar misconduct, and raises questions as to whether the FTC is engaging in disparate treatment based on business size and type, rather than on facts and evidence.

In 2014, the FTC charged Ajay Prasad, Shreekant Srivastava, and their company, GMR Transcription Services, with violating the FTC Act’s prohibition on unfair practices when it failed to ensure its vendors protected sensitive data. As detailed in the Commission’s complaint, GMR failed to ensure that their vendors implemented reasonable security measures, and failed to prevent one vendor from storing sensitive files in plain text. The complaint does not allege that malicious actors attacked the vendor’s systems, nor does it allege that GMR’s failure to oversee the vendor directly led to the improper data disclosure, but nevertheless charges both the firm and its owners with engaging in unfair business practices by failing to employ reasonable security measures.¹⁵

If GMR faced this scrutiny, why wouldn’t Ascension? The FTC’s complaint alleged that GMR’s lax policies created a vulnerability that was exploited at least once, and the FTC’s complaint in this matter details some of the consequences of this catastrophic breach, which involved dozens of actors, mainly from overseas, including those with IP addresses in China and Russia. They were able to access more than 60,000 Americans’ sensitive financial information. Furthermore, in failing to prevent this mass theft, Ascension disregarded its own risk management policies, failing to take “any of the steps described in its own policy to evaluate [its vendors’] security practices.”¹⁶

¹³ *Fed. Trade Comm’n v. Wyndham et al.*, 2013 WL 11116791 (D.N.J. May 20, 2013).

¹⁴ *Fed. Trade Comm’n v. Wyndham Worldwide Corp.*, 2014 WL 2812049, at *7 (D.N.J. June 23, 2014).

¹⁵ Compl., *In the Matter of GMR Transcription Services, Inc.*, Fed. Trade Comm’n File No. 1223095 (Aug. 21, 2014), <https://www.ftc.gov/system/files/documents/cases/140821gmrcmpt.pdf>.

¹⁶ Compl., *In the Matter of Ascension Data & Analytics, LLC*, Fed. Trade Comm’n File No. 1923126.

Dissenting Statement

Taken together, the allegations against Ascension leave little doubt that the company's practices were unfair, causing far more unavoidable injury than GMR, without any apparent benefit to consumers or competition.¹⁷ When the Commission settled with GMR, the law was exactly the same. The only thing that changed is the five members of the Commission.

My colleague suggests there are questions about whether Ascension's practices were unfair, but the Commission's complaint details how elementary the missteps were that led to this breach. A reasonable person would expect if these problems could have been prevented simply by Ascension following its own vendor management policies. Ascension could have also heeded the FTC's 2015 business guidance, which warns firms to "[m]ake sure service providers implement reasonable security measures."¹⁸

My colleague also cites instances where the Commission has charged a firm with violating the FTC's Safeguards Rule without also including charges of unfair practices. However, these cases do not involve conduct related to inadequate service provider oversight, which is the core allegation at issue with Rocktop and Ascension.

We must apply more evenhanded enforcement to ensure that large businesses and investment firms are not getting less scrutiny than small businesses. The Commission's failure to charge Ascension and its affiliates with an unfairness violation is not only inconsistent with prior practice but also undermines our ability to hold the company accountable for its failures.

Rethinking Remedies

The most effective way to address serious data breaches like this one is to compensate the victims, penalize the wrongdoers, and insist on changes to the responsible company's practices. Unfortunately, the Commission's proposed order misses the mark on identifying the responsible company, while doing nothing to compensate victims or penalize those responsible for this catastrophic breach. I am therefore not confident that the remedies proposed in today's order will deter other companies from engaging in the same slipshod practices.

We could have done more. I recognize that consumers harm can be difficult to estimate in these cases, and that the Commission lacks civil penalty authority for offenses like this one. But that problem can be solved. The FTC is not the only enforcer in this space – dozens of state attorneys general and financial regulators can enforce a nearly identical unfairness authority under federal law that is backed up with strong tools to both seek redress and penalties. By partnering with a state enforcer, the Commission can dramatically improve its data security actions – ensuring that there is compensation for victims and consequences for wrongdoing.¹⁹

¹⁷ See 15 U.S.C. § 45n Defining as unfair practices that cause or are likely to cause substantial injury that is not reasonably avoidable, and is not outweighed by benefits to consumers or competition.

¹⁸ START WITH SECURITY, A GUIDE FOR BUSINESS, LESSONS LEARNED FROM FTC CASES, FED. TRADE COMM'N (Jun. 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

¹⁹ In addition to having unfairness jurisdiction, many state enforcers have their own versions of the Safeguards Rule. See, e.g., *Industry Guidance Re: Standards for Safeguarding Customer Information and Regulation 173*, NEW YORK STATE DEP'T OF FIN. SERV., <https://www.dfs.ny.gov/insurance/ogco2002/rg204021.htm>.

Concurring Statement

Unfortunately, the FTC almost never invites state regulators, particularly state banking regulators with significant expertise, to join our investigations and enforcement actions to obtain additional relief when it comes to data protection. This must change.

Conclusion

We should all be unconvinced that chasing after dangerous data breaches and resolving them without any redress or penalties is an effective strategy. Making matters worse, holding a “company” accountable that is really just an extension of a financial firm might allow our order to be completely ignored. After this settlement, Ascension could “fold,” and the Rocktop family of companies can reconstitute it, escaping any obligations under the order.¹

The FTC is currently considering changes to its rule on safeguarding consumer financial information.² But, we also need to rethink our enforcement strategy. Our go-it-alone strategy is doing nothing for breach victims and little to deter, and our two-track approach to unfairness is penalizing small companies while giving a pass to financial firms like Rocktop. For these reasons, I respectfully dissent.

STATEMENT OF COMMISSIONER NOAH JOSHUA PHILLIPS

December 15, 2020

The Commission today announced our most recent settlement resolving an alleged violation of the Gramm-Leach-Bliley Safeguards Rule (“Rule”), a critical facet of the Commission’s data privacy and security enforcement program. According to the complaint, Ascension Data & Analytics (“Ascension”) violated the Rule by failing to vet properly and oversee a provider of optical character recognition (OCR) services, and by failing to conduct appropriate risk assessments. This settlement requires Ascension to implement a comprehensive data security program including annual third-party assessments.

I write to address several points in Commissioner Chopra’s dissenting statement.

¹ For context, public information indicates that there are seven companies with interrelated officers or agents currently active, including “Reidpin LLC,” “Reidpin, LLC,” “Reidpin Investments, LLC,” Reidpin Rocktop 1, LLC,” “Reidpin Rocktop III, LLC,” “Reidpin Rocktop IV, LLC,” “Reidpin Rocktop V, LLC” founded in 2011, 2014, 2015, 2016, two in 2017, and one in 2018. There are two other entities with these characteristics which appear to have folded. <https://opencorporates.com/companies?q=REIDPIN%2C+LLC>.

² Fed. Trade Comm’n., Standards on Safeguarding Customer Information, 84 Fed. Reg. 13158 (Apr. 4, 2019), <https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information>.

Dissenting Statement

Commissioner Chopra dissents because he believes the Commission should name Rocktop Partners, a company in the same corporate family as Ascension, as a respondent. Commissioner Chopra points to corporate affiliation and certain overlaps in management and facilities between the two firms, and other entities as well. It is not clear under what legal theory—whether veil piercing, common enterprise, or the like—he would name other defendants; but, without more, the facts alleged do not support doing so.³

In terms of relief, Commissioner Chopra argues that Rocktop will dissolve Ascension and set up a new firm or transfer its functions, just to avoid its obligations under the settlement. This is the kind of conduct characteristic of boiler rooms and other frauds. It is not clear to me why Rocktop—an entity regulated by the Securities and Exchange Commission—would dissolve and reconstitute an affiliate for the sole purpose of failing to oversee vendors, or otherwise evading this order.⁴

Commissioner Chopra also would have the Commission allege that Ascension’s conduct was unfair. In the Gramm-Leach-Bliley (GLB) Act, Congress gave us a specialized data security statute, and the Safeguards Rule, promulgated pursuant to that Act, establishes liability under the facts alleged in this case.⁵ We should use that authority, and here we are. I do not see what an additional allegation of unfairness would achieve—certainly, no change in the remedy, and nothing better for consumers. What is more, when pleading that lax data security was unfair under Section 5, we need evidence to satisfy the unfairness test; that gets into thornier questions of whether the oversight failure here can constitute unfairness. Thanks to GLB, we need not answer that.

Commissioner Chopra claims that Ascension is being favored because, in the Commission’s 2014 case against GMR Transcription Services, it pleaded an unfairness count. He attributes the difference in treatment to the small size of the respondent in that case. GMR was not a financial services firm, however, so the Commission could not have alleged a violation of the GLB Safeguards Rule in that case; and the respondent in this case, Ascension, is also a small

³ For example, Commissioner Chopra cites no facts to suggest that corporate formalities were not observed, that Ascension is under-capitalized, or that corporate form was abused to inoculate Rocktop from liability (mind the reader, for Ascension’s failure to oversee a vendor) to justify piercing the corporate veil. Courts generally take a dim view of piercing the corporate veil without a substantial basis to do so. *See, e.g., Trinity Indus., Inc. v. Greenlease Holding Co.*, 903 F.3d 333, 365 (3d Cir. 2018) (“the corporate veil may be pierced only in extraordinary circumstances, such as when the corporate form would otherwise be misused to accomplish certain wrongful purposes”) (internal citations and quotations omitted). And for good reason: the ability to make investments without risk of liability is foundational to the American legal and economic system.

⁴ Commissioner Chopra cites *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887 (ES), 2014 WL 2812049, at *8 (D.N.J. June 23, 2014), for the proposition that companies other than frauds may reorganize in an effort to avoid responsibilities under FTC orders. Of course that is true, but that does not mean that every entity in a corporate family can or should be bound by every FTC order. And, certainly, that is not what the court—considering a motion to dismiss—held in that case.

⁵ 15 U.S.C. § 6801 *et seq.*; 16 C.F.R. Part 314. The limits of applying Section 5 to data security cases are precisely why the Commission, on a bipartisan basis, seeks data security legislation from Congress.

Concurring Statement

company. It is not at all unusual for the Commission to charge a violation of the Safeguards Rule without an accompanying unfairness count.⁶

This is a strong case and a good result. I commend Staff for its thoughtful and energetic efforts to use the authority at our disposal to protect American consumers

**DISSENTING STATEMENT OF
COMMISSIONER REBECCA KELLY SLAUGHTER**
December 22, 2021

The Commission is finalizing an order resolving Ascension Data & Analytics, LLC's alleged violations of the Commission's Standards for Safeguarding Customer Information Rule ("Safeguards Rule"). Ascension is an analytics company that provides data, analytics, and system-based technology services and products to other companies in its corporate family in connection with mortgages. The FTC's complaint alleges that Ascension failed to oversee its vendors or adequately assess risk to ensure that customer data was secure. One of Ascension's vendors had a major security failure that exposed the personal data of tens of thousands of individuals for many months.¹

According to the FTC's complaint, Ascension did not even fulfill the basic due diligence and oversight steps required by its own risk management policies.² Such fundamental failings and lack of care for sensitive personal data is not just a violation of the Safeguards Rule, it is also an unfair practice under Section 5 of the FTC Act.³ Yet, the proposed complaint alleges *only* a rule violation and does not charge an unfairness violation of Section 5.

⁶ See, e.g., *TaxSlayer, LLC*, No. C-4626 (Nov. 8, 2017), <https://www.ftc.gov/enforcement/cases-proceedings/162-3063/taxslayer>; *James B. Nutter & Co.*, No. C-4258 (June 16, 2009), <https://www.ftc.gov/enforcement/casesproceedings/072-3108/james-b-nutter-company-corporation-matter>; *United States v. American United Mortgage Co.*, No. 07-cv-7064 (N.D. Ill.), <https://www.ftc.gov/enforcement/cases-proceedings/062-3103/american-united-mortgagecompany-united-states-america-ftc>. I am unaware of any case where we alleged a failure to oversee as a violation of *both* GLB and Section 5, as Commissioner Chopra would have us do here.

¹ See Compl. ¶¶ 3, 9-10, 14-21, *In the Matter of Ascension Data & Analytics, LLC* (Dec. 15, 2020), <https://www.ftc.gov/system/files/documents/cases/1923126ascensioncomplaint.pdf>.

² Compl. ¶¶ 7-8, 15-16, 20-21.

³ Pleading unfairness in data security cases where a company fails to take steps to ensure that its contractors safeguard personal data is not novel. In 2014, the Commission alleged that GMR Transcription Services' failure to require and verify that its independent service providers implemented reasonable security measures was an unfair practice in violation of Section 5. See, Compl., *In the Matter of GMR Transcription Services, Inc.*, (Aug. 21, 2014), <https://www.ftc.gov/system/files/documents/cases/140821gmrempt.pdf>.

Analysis to Aid Public Comment

I have consistently argued that when the FTC fails to plead all relevant law violations—particularly unfairness—we miss important opportunities to establish the scope of behavior that is covered by the general statutes we enforce.¹ Especially to the extent that our enforcement program is driven by negotiated consents rather than litigated orders or duly promulgated rules, our consents are extremely important for market participants to understand how particular conduct violates the law. In other words, every time the Commission files a complaint we send a signal to industry about what constitutes a law violation.

Failure to adequately vet and oversee vendors entrusted with sensitive personal information is unlawful not just for financial institutions covered by the Safeguards Rule, but for all companies governed by the FTC Act. I believe the facts here support a count of unfairness under Section 5, as well as Safeguards Rule violations. Because this action fails to fully plead the violations supported by the facts and the law in this case, I respectfully dissent.

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission (“Commission”) has accepted, subject to final approval, an agreement containing a consent order from Ascension Data & Analytics, LLC (“Respondent”).

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

Respondent is a Delaware company with its principal place of business in Texas. Respondent provides data, analytics, and technology services to other companies in its corporate family and their service providers relating to residential mortgages.

In early 2017, as part of work for a related company, Respondent hired a vendor to conduct Optical Character Recognition on a set of documents pertaining to 37,000 residential mortgages. The documents contained the personal information of 60,593 consumers. The type of personal information included names, dates of birth, Social Security numbers, loan information, credit and debit account numbers, drivers’ license numbers, and credit files. Before providing the documents to the vendor, Respondent did not take steps to make sure the vendor was capable of protecting

¹ See, e.g., FTC Data Privacy Enforcement: A Time of Change; Dissenting Statement of Commissioner Rebecca Kelly Slaughter Regarding FTC v. Progressive Leasing; Concurring Statement of Commissioner Rebecca Kelly Slaughter Regarding Vyera Pharmaceuticals.

Analysis to Aid Public Comment

the personal information in the documents. Furthermore, Respondent did not require the vendor by contract to protect the documents or the consumer information contained therein.

From January 2018 to January 2019, the vendor inadvertently exposed the information from the mortgage documents online, by misconfiguring a cloud server and storage location containing information from the documents. As a result, anyone who could figure out the web address of the server or storage location could view and download the contents. The server and storage location were accessed by fifty-two unauthorized computers during the year they were exposed.

The Commission's proposed one-count complaint alleges that Respondent violated the Standards for Safeguarding Customer Information Rule ("Safeguards Rule") of the Gramm-Leach-Bliley Act ("GLB Act"). The Safeguards Rule requires financial institutions, which includes companies like Respondent, to implement a comprehensive information security program that contains certain elements.

The proposed complaint alleges that Respondent violated the Safeguards Rule by failing to include two of the required elements in its information security program. First, the proposed complaint alleges, Respondent did not oversee service providers, by failing to take reasonable steps to choose service providers capable of safeguarding personal information, and failing to require those service providers by contract to maintain the safeguards. Second, the proposed complaint alleges, Respondent failed to identify risks to the security of personal information, and assess whether any safeguards it had in place were sufficient. Respondent did not satisfy this element of the Safeguards Rule because it failed to consider risks related to many service providers, and did not conduct risk assessments before September 2017.

The Proposed Order contains provisions designed to prevent Respondent from engaging in the same or similar acts or practices in the future. Part I of the Proposed Order prohibits Respondent from violating the Safeguards Rule.

Part II of the Proposed Order requires Respondent to establish and implement, and thereafter maintain, a comprehensive data security program that protects the security of Covered Information, the definition of which is modeled off the definitions of the Safeguards Rule.

Part III of the Proposed Order requires Respondent to obtain initial and biennial data security assessments for ten years.

Part IV of the Proposed Order requires Respondent to disclose all material facts to the assessor and prohibits Respondent from misrepresenting any fact material to the assessments required by Part III.

Part V of the Proposed Order requires Respondent to submit an annual certification from a senior corporate manager (or senior officer responsible for its data security program) that Respondent has implemented the requirements of the Order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Analysis to Aid Public Comment

Part VI of the Proposed Order requires Respondent to notify the Commission any time it is required to make a notification to a state or local government that personal information has been breached or disclosed.

Parts VII through X of the Proposed Order are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondent to provide information or documents necessary for the Commission to monitor compliance. Part XI states that the Proposed Order will remain in effect for 20 years, with certain exceptions.

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.

INTERLOCUTORY, MODIFYING, VACATING, AND MISCELLANEOUS ORDERS

IN THE MATTER OF

HACKENSACK MERIDIAN HEALTH, INC.

AND

ENGLEWOOD HEALTHCARE FOUNDATION

Docket No. 9399. Order, July 1, 2021

Order granting the joint expedited motion for a continuance of Administrative Proceedings.

ORDER GRANTING FURTHER CONTINUANCE

On June 23, 2021, Complaint Counsel and Respondents Hackensack Meridian Health, Inc. (“HMH”) and Englewood Healthcare Foundation (“Englewood”) jointly moved to postpone commencement of the evidentiary hearing in this proceeding by approximately thirty days, until August 16, 2021. Joint Expedited Motion for a Continuance of Administrative Proceedings (“Joint Motion”). This represents the second joint request for continuance of the evidentiary hearing. On May 25, 2021, we granted a similar joint motion to continue the commencement of the hearing from June 15, 2021 to July 15, 2021. Order Granting Continuance (“May 25 Order”). For reasons similar to those expressed in our May 25 Order, we have determined to grant a further continuance of the hearing to August 16, 2021.

On December 3, 2020, the Commission issued an administrative complaint challenging a proposed transaction whereby HMH would acquire Englewood (“the Proposed Transaction”). The Commission at that time also filed a complaint in the U.S. District Court for the District of New Jersey seeking a preliminary injunction barring the Proposed Transaction until completion of the administrative proceeding. The preliminary injunction hearing concluded on May 18, 2021, and the district court heard closing arguments on June 2, 2021. The parties anticipate receiving a decision in that action within the next several months. Joint Motion at 2. The parties state that “[i]t is highly likely that [the preliminary injunction] ruling will cause these administrative proceedings to be suspended or rendered moot.” *Id.* at 4.

The parties argue that granting the requested continuance and extending pre-hearing deadlines would protect the parties and third parties and their witnesses from unnecessary burdens and expense, without prejudicing the Commission. *Id.* at 1-4. They explain that third parties will need to prepare complex submissions seeking in camera treatment of their discovery materials, and that witnesses – including up to 28 third-party witnesses – face the burden, expense, and disruption of preparing to testify and testifying. *Id.* at 3. *See* May 25 Order at 1-2.